



HiveForce Labs

**CISA**

**KNOWN**

**EXPLOITED**

**VULNERABILITY**

**CATALOG**

**September 2026**

# Table of Contents

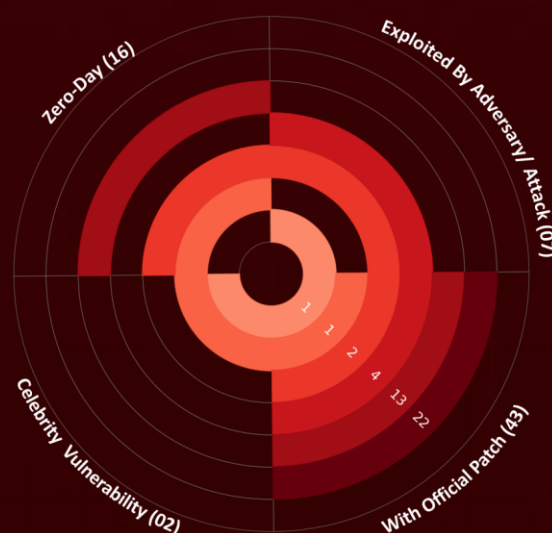
|                        |    |
|------------------------|----|
| <u>Summary</u>         | 03 |
| <u>CVEs List</u>       | 04 |
| <u>CVEs Details</u>    | 13 |
| <u>Recommendations</u> | 53 |
| <u>References</u>      | 54 |
| <u>Appendix</u>        | 54 |
| <u>What Next?</u>      | 55 |

# Summary

The Known Exploited Vulnerability (KEV) catalog, maintained by CISA, is the authoritative source of vulnerabilities that have been exploited in the wild.

It is recommended that all organizations review and monitor the KEV catalog, prioritize remediation of listed vulnerabilities, and reduce the likelihood of compromise by threat actors. In **September 2026**, **43** vulnerabilities met the criteria for inclusion in CISA's KEV catalog. Of these, **16** are **zero-day** vulnerabilities; **7** have been **exploited** by a threat actor and employed in attacks.

**43**  
Known Exploited  
Vulnerabilities





# CVEs List

| CVE                            | NAME                                                                                                   | AFFECTED PRODUCT              | CVSS 3.x SCORE | ZERO-DAY | PATCH | DUE DATE           |
|--------------------------------|--------------------------------------------------------------------------------------------------------|-------------------------------|----------------|----------|-------|--------------------|
| CVE-2026-76504                 | Cisco Catalyst SD-WAN Manager Hex Encoding Vulnerability                                               | Cisco Catalyst SD-WAN Manager | 9.8            |          |       | October 03, 2026   |
| <a href="#">CVE-2026-86950</a> | Apple Multiple Products Out-of-Bounds Write Vulnerability                                              | Apple Multiple Products       | 8.8            |          |       | October 02, 2026   |
| <a href="#">CVE-2026-88772</a> | Citrix NetScaler Improper Restriction of Operations within the Bounds of a Memory Buffer Vulnerability | Citrix NetScaler              | 8.1            |          |       | September 30, 2026 |
| <a href="#">CVE-2026-88771</a> | Citrix NetScaler Improper Input Validation Vulnerability                                               | Citrix NetScaler              | 9.8            |          |       | September 30, 2026 |

| CVE                            | NAME                                                                        | AFFECTED PRODUCT              | CVSS 3.x SCORE | ZERO-DAY                                                                            | PATCH                                                                                 | DUE DATE           |
|--------------------------------|-----------------------------------------------------------------------------|-------------------------------|----------------|-------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------|--------------------|
| CVE-2026-67279                 | Mikrotik RouterOS Improper Enforcement of Behavioral Workflow Vulnerability | MikroTik RouterOS             | 6.5            |    |    | September 28, 2026 |
| CVE-2026-65660                 | Microsoft SharePoint Code Injection Vulnerability                           | Microsoft SharePoint          | 8.8            |    |    | September 28, 2026 |
| <a href="#">CVE-2026-87902</a> | WordPress Core Remote File Inclusion Vulnerability                          | WordPress Core                | 8.1            |    |    | September 28, 2026 |
| CVE-2026-5430                  | WSO2 Multiple Products Path Traversal Vulnerability                         | WSO2 Multiple Products        | 10             |  |  | September 27, 2026 |
| CVE-2026-71362                 | Adobe Commerce and Magento Incorrect Authorization Vulnerability            | Adobe Commerce and Magento    | 9.1            |  |  | September 27, 2026 |
| <a href="#">CVE-2026-93952</a> | Arista VeloCloud Orchestrator Improper Input Validation Vulnerability       | Arista VeloCloud Orchestrator | 10             |  |  | September 25, 2026 |

| CVE                            | NAME                                                                        | AFFECTED PRODUCT              | CVSS 3.x SCORE | ZERO-DAY                                                                            | PATCH                                                                                 | DUE DATE           |
|--------------------------------|-----------------------------------------------------------------------------|-------------------------------|----------------|-------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------|--------------------|
| <a href="#">CVE-2026-94127</a> | F5 BIG-IP APM Heap-based Buffer Overflow Vulnerability                      | F5 BIG-IP APM                 | 9.8            |    |    | September 25, 2026 |
| <a href="#">CVE-2026-93616</a> | Check Point Multiple Products Path Traversal Vulnerability                  | Check Point Multiple Products | 9.8            |    |    | September 25, 2026 |
| <a href="#">CVE-2026-85102</a> | Check Point Multiple Products Improper Certificate Validation Vulnerability | Check Point Multiple Products | 9.8            |    |    | September 25, 2026 |
| <a href="#">CVE-2026-7273</a>  | Zyxel GS1900 Series Switches Stack-Based Buffer Overflow Vulnerability      | Zyxel GS1900 Series Switches  | 8.8            |  |  | September 24, 2026 |
| <a href="#">CVE-2025-39964</a> | Linux Kernel Race Condition Vulnerability                                   | Linux Kernel                  | 5.5            |  |  | September 21, 2026 |
| <a href="#">CVE-2026-53266</a> | Linux Kernel Out-of-Bounds Write Vulnerability                              | Linux Kernel                  | 8.8            |  |  | September 21, 2026 |

| CVE                            | NAME                                                                            | AFFECTED PRODUCT               | CVSS 3.x SCORE | ZERO-DAY                                                                            | PATCH                                                                                 | DUE DATE           |
|--------------------------------|---------------------------------------------------------------------------------|--------------------------------|----------------|-------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------|--------------------|
| CVE-2025-39682                 | Linux Kernel Improper Check for Unusual or Exceptional Conditions Vulnerability | Linux Kernel                   | 9.8            |    |    | September 21, 2026 |
| CVE-2026-58704                 | Google Pixel Improper Authorization Vulnerability                               | Google Pixel                   | 8.8            |    |    | September 19, 2026 |
| <a href="#">CVE-2026-76460</a> | Cisco Identity Services Engine Incorrect Use of Privileged APIs Vulnerability   | Cisco Identity Services Engine | 10             |    |    | September 19, 2026 |
| <a href="#">CVE-2026-87886</a> | Acronis Backup Incorrect Default Permissions Vulnerability                      | Acronis Backup                 | 7.8            |  |  | September 19, 2026 |
| <a href="#">CVE-2026-76461</a> | Cisco Secure Email Gateway SQL Injection Vulnerability                          | Cisco Secure Email Gateway     | 9.8            |  |  | September 17, 2026 |

| CVE                            | NAME                                                                                            | AFFECTED PRODUCT                                | CVSS 3.x SCORE | ZERO-DAY                                                                            | PATCH                                                                                 | DUE DATE           |
|--------------------------------|-------------------------------------------------------------------------------------------------|-------------------------------------------------|----------------|-------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------|--------------------|
| <a href="#">CVE-2026-84869</a> | ConnectWise ScreenConnect Improper Privilege Management and Missing Authorization Vulnerability | ConnectWise ScreenConnect                       | 9.9            |    |    | September 14, 2026 |
| <a href="#">CVE-2026-42016</a> | JFrog Artifactory Incorrect Authorization Vulnerability                                         | JFrog Artifactory                               | 8.8            |    |    | September 25, 2026 |
| <a href="#">CVE-2026-42018</a> | JFrog Artifactory Improper Authentication Vulnerability                                         | JFrog Artifactory                               | 7.5            |  |  | September 25, 2026 |
| <a href="#">CVE-2026-85706</a> | GitLab Community Edition and Enterprise Edition Path Traversal Vulnerability                    | GitLab Community Edition and Enterprise Edition | 10             |  |  | September 14, 2026 |

| CVE            | NAME                                                                                        | AFFECTED PRODUCT           | CVSS 3.x SCORE | ZERO-DAY                                                                            | PATCH                                                                                 | DUE DATE           |
|----------------|---------------------------------------------------------------------------------------------|----------------------------|----------------|-------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------|--------------------|
| CVE-2026-86060 | MikroTik RouterOS Improper Neutralization of Argument Delimiters in a Command Vulnerability | MikroTik RouterOS          | 9.8            |    |    | September 13, 2026 |
| CVE-2026-67277 | MikroTik RouterOS Missing Authentication for Critical Function Vulnerability                | MikroTik RouterOS          | 8.2            |    |    | September 13, 2026 |
| CVE-2026-19490 | Citrix NetScaler Authentication Bypass Using an Alternate Path or Channel Vulnerability     | Citrix NetScaler           | 9.8            |  |  | September 12, 2026 |
| CVE-2025-25249 | Fortinet Multiple Products Heap-based Buffer Overflow Vulnerability                         | Fortinet Multiple Products | 9.8            |  |  | September 12, 2026 |

| CVE                            | NAME                                                                                                           | AFFECTED PRODUCT                                                                                   | CVSS 3.x SCORE | ZERO-DAY                                                                            | PATCH                                                                                 | DUE DATE           |
|--------------------------------|----------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------|----------------|-------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------|--------------------|
| <a href="#">CVE-2026-87491</a> | Google Chromium V8 Out of Bounds Write Vulnerability                                                           | Google Chromium V8                                                                                 | 8.8            |    |    | September 23, 2026 |
| CVE-2026-20079                 | Cisco Firewall Management Center Authentication Bypass Using an Alternate Path or Channel Vulnerability        | Cisco Secure Firewall Management Center (FMC) and Security Cloud Control (SCC) Firewall Management | 10             |    |    | September 12, 2026 |
| <a href="#">CVE-2026-75650</a> | Adobe Commerce and Magento Improper Neutralization of Special Elements Used in a Template Engine Vulnerability | Adobe Commerce and Magento                                                                         | 10             |  |  | September 11, 2026 |
| <a href="#">CVE-2026-81963</a> | Microsoft Windows Link Following Vulnerability                                                                 | Microsoft Windows                                                                                  | 7.8            |  |  | September 22, 2026 |

| CVE                            | NAME                                                           | AFFECTED PRODUCT   | CVSS 3.x SCORE | ZERO-DAY                                                                            | PATCH                                                                                 | DUE DATE           |
|--------------------------------|----------------------------------------------------------------|--------------------|----------------|-------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------|--------------------|
| <a href="#">CVE-2026-86218</a> | N-able N-central Static Code Injection Vulnerability           | N-able N-central   | 8.8            |    |    | September 11, 2026 |
| <a href="#">CVE-2026-85880</a> | Microsoft Windows Heap-Based Buffer Overflow Vulnerability     | Microsoft Windows  | 8.2            |    |    | September 22, 2026 |
| <a href="#">CVE-2026-85046</a> | Google Chromium V8 Type Confusion Vulnerability                | Google Chromium V8 | 10             |    |    | September 18, 2026 |
| CVE-2026-59822                 | BerriAI LiteLLM Improper Authentication Vulnerability          | BerriAI LiteLLM    | 9.8            |  |  | September 16, 2026 |
| <a href="#">CVE-2026-48710</a> | Kludex Starlette HTTP Request/Response Smuggling Vulnerability | Kludex Starlette   | 6.5            |  |  | September 16, 2026 |
| CVE-2026-49869                 | Kestra OSS OS Command Injection Vulnerability                  | Kestra Kestra OSS  | 7.8            |  |  | September 05, 2026 |

| CVE                            | NAME                                                                   | AFFECTED PRODUCT             | CVSS 3.x SCORE | ZERO-DAY                                                                            | PATCH                                                                                 | DUE DATE           |
|--------------------------------|------------------------------------------------------------------------|------------------------------|----------------|-------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------|--------------------|
| <a href="#">CVE-2026-82329</a> | JFrog Artifactory Improper Authentication Vulnerability                | JFrog Artifactory            | 9.8            |    |    | September 05, 2026 |
| CVE-2026-9586                  | Sangoma Switchvox SQL Injection Vulnerability                          | Sangoma Switchvox            | 9.8            |    |    | September 05, 2026 |
| <a href="#">CVE-2026-83548</a> | SonicWall SMA1000 Appliances Server-Side Request Forgery Vulnerability | SonicWall SMA1000 Appliances | 10             |    |    | September 05, 2026 |
| <a href="#">CVE-2026-83549</a> | SonicWall SMA1000 Appliances OS Command Injection Vulnerability        | SonicWall SMA1000 Appliances | 7.8            |  |  | September 05, 2026 |



CVEs Details

| CVE ID                                                   | CELEBRITY VULNERABILITY                                                           | AFFECTED PRODUCTS                                                                                               | ASSOCIATED ACTOR                                                                                                                                                                                                                          |
|----------------------------------------------------------|-----------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| CVE-2026-76504                                           |  | Cisco Catalyst SD-WAN Manager before 20.9.10.1, 20.12.8.2, 20.15.6.1, 20.18.4.1, and 26.1.2.1, and version 26.2 | -                                                                                                                                                                                                                                         |
|                                                          | ZERO-DAY                                                                          |                                                                                                                 |                                                                                                                                                                                                                                           |
|                                                          |  | AFFECTED CPE                                                                                                    | ASSOCIATED ATTACKS/RANSOMWARE                                                                                                                                                                                                             |
| NAME                                                     | BAS ATTACKS                                                                       | cpe:2.3:a:cisco:catalyst_sd-wan_manager:*:*:*:*:*:*                                                             | -                                                                                                                                                                                                                                         |
| Cisco Catalyst SD-WAN Manager Hex Encoding Vulnerability |  |                                                                                                                 |                                                                                                                                                                                                                                           |
|                                                          | CWE ID                                                                            | ASSOCIATED TTPs                                                                                                 | PATCH LINK                                                                                                                                                                                                                                |
|                                                          | CWE-177                                                                           | T1190: Exploit Public-Facing Application, T1068: Exploitation for Privilege Escalation                          | <a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sdwan-webauth-xr8beuuU">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sdwan-webauth-xr8beuuU</a> |

| CVE ID                                                    | CELEBRITY VULNERABILITY                                                           | AFFECTED PRODUCTS                                                                                                  | ASSOCIATED ACTOR                                                                                                                                                                                                                                                                              |
|-----------------------------------------------------------|-----------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <u>CVE-2026-86950</u>                                     |  | Apple iOS and iPadOS before 26.7.1, macOS Sequoia before 15.8.1, and macOS Tahoe before 26.7.1                     | -                                                                                                                                                                                                                                                                                             |
|                                                           | ZERO-DAY                                                                          |                                                                                                                    |                                                                                                                                                                                                                                                                                               |
|                                                           |  | AFFECTED CPE                                                                                                       | ASSOCIATED ATTACKS/RANSOMWARE                                                                                                                                                                                                                                                                 |
| NAME                                                      | BAS ATTACKS                                                                       | cpe:2.3:o:apple:ipados:*:*:*:*:*:*:*<br>cpe:2.3:o:apple:iphone_os:*:*:*:*:*:*<br>cpe:2.3:o:apple:macos:*:*:*:*:*:* | -                                                                                                                                                                                                                                                                                             |
| Apple Multiple Products Out-of-Bounds Write Vulnerability |  |                                                                                                                    |                                                                                                                                                                                                                                                                                               |
|                                                           | CWE ID                                                                            | ASSOCIATED TTPs                                                                                                    | PATCH LINK                                                                                                                                                                                                                                                                                    |
|                                                           | CWE-787                                                                           | T1203: Exploitation for Client Execution, T1204.002: User Execution: Malicious File                                | <a href="https://support.apple.com/en-us/149226">https://support.apple.com/en-us/149226</a> ,<br><a href="https://support.apple.com/en-us/149228">https://support.apple.com/en-us/149228</a> ,<br><a href="https://support.apple.com/en-us/149229">https://support.apple.com/en-us/149229</a> |

| CVE ID                                                                                                 | CELEBRITY VULNERABILITY                                                           | AFFECTED PRODUCTS                                                                                                                                                                                    | ASSOCIATED ACTOR                                                                                                                                                                |
|--------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <u>CVE-2026-88772</u>                                                                                  |  | Citrix NetScaler ADC before 14.1-73.37 and 13.1-64.23, NetScaler ADC FIPS before 14.1-73.37, NetScaler ADC FIPS and NDcPP before 13.1-37.279, and NetScaler Gateway before 14.1-73.37 and 13.1-64.23 | -                                                                                                                                                                               |
|                                                                                                        | ZERO-DAY                                                                          |                                                                                                                                                                                                      |                                                                                                                                                                                 |
|                                                                                                        |  | AFFECTED CPE                                                                                                                                                                                         | ASSOCIATED ATTACKS/RANSOMWARE                                                                                                                                                   |
| NAME                                                                                                   | BAS ATTACKS                                                                       | cpe:2.3:a:citrix:netScaler_application_delivery_controller:*:*:*:*:*:*:*<br>cpe:2.3:a:citrix:netScaler_gateway:*:*:*:*:*:*:*                                                                         | -                                                                                                                                                                               |
| Citrix NetScaler Improper Restriction of Operations within the Bounds of a Memory Buffer Vulnerability |  |                                                                                                                                                                                                      |                                                                                                                                                                                 |
|                                                                                                        | CWE ID                                                                            | ASSOCIATED TTPs                                                                                                                                                                                      | PATCH LINK                                                                                                                                                                      |
|                                                                                                        | CWE-119                                                                           | T1190: Exploit Public-Facing Application, T1499.004: Endpoint Denial of Service: Application or System Exploitation                                                                                  | <a href="https://support.citrix.com/support-home/kbsearch/article?articleNumber=CTX697096">https://support.citrix.com/support-home/kbsearch/article?articleNumber=CTX697096</a> |

| CVE ID                                                   | CELEBRITY VULNERABILITY                                                           | AFFECTED PRODUCTS                                                                                                                                                                                    | ASSOCIATED ACTOR                                                                                                                                                                |
|----------------------------------------------------------|-----------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <u>CVE-2026-88771</u>                                    |  | Citrix NetScaler ADC before 14.1-73.37 and 13.1-64.23, NetScaler ADC FIPS before 14.1-73.37, NetScaler ADC FIPS and NDcPP before 13.1-37.279, and NetScaler Gateway before 14.1-73.37 and 13.1-64.23 | -                                                                                                                                                                               |
|                                                          | ZERO-DAY                                                                          |                                                                                                                                                                                                      |                                                                                                                                                                                 |
|                                                          |  | AFFECTED CPE                                                                                                                                                                                         | ASSOCIATED ATTACKS/RANSOMWARE                                                                                                                                                   |
| NAME                                                     | BAS ATTACKS                                                                       | cpe:2.3:a:citrix:netcaler_application_delivery_controller:*:*:*:*:*:*:*<br>cpe:2.3:a:citrix:netcaler_gateway:*:*:*:*:*:*:*                                                                           | -                                                                                                                                                                               |
| Citrix NetScaler Improper Input Validation Vulnerability |  |                                                                                                                                                                                                      |                                                                                                                                                                                 |
|                                                          | CWE ID                                                                            | ASSOCIATED TTPs                                                                                                                                                                                      | PATCH LINK                                                                                                                                                                      |
|                                                          | CWE-20                                                                            | T1190: Exploit Public-Facing Application, T1059: Command and Scripting Interpreter                                                                                                                   | <a href="https://support.citrix.com/support-home/kbsearch/article?articleNumber=CTX697096">https://support.citrix.com/support-home/kbsearch/article?articleNumber=CTX697096</a> |

| CVE ID                                                                      | CELEBRITY VULNERABILITY                                                           | AFFECTED PRODUCTS                                                                                                                                                    | ASSOCIATED ACTOR                                                                                                                          |
|-----------------------------------------------------------------------------|-----------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------|
| CVE-2026-67279                                                              |  | MikroTik RouterOS before 6.49.21 (long-term), 7.23.4 (long-term), and 7.24.2 (stable)                                                                                | -                                                                                                                                         |
|                                                                             | ZERO-DAY                                                                          |                                                                                                                                                                      |                                                                                                                                           |
|                                                                             |  | AFFECTED CPE                                                                                                                                                         | ASSOCIATED ATTACKS/RANSOMWARE                                                                                                             |
| NAME                                                                        | BAS ATTACKS                                                                       | cpe:2.3:o:mikrotik:routeros:*:*:*.*.*.*.*                                                                                                                            | -                                                                                                                                         |
| Mikrotik RouterOS Improper Enforcement of Behavioral Workflow Vulnerability |  |                                                                                                                                                                      |                                                                                                                                           |
|                                                                             | CWE ID                                                                            | ASSOCIATED TTPs                                                                                                                                                      | PATCH LINK                                                                                                                                |
|                                                                             | CWE-841                                                                           | T1190: Exploit Public-Facing Application, T1136.001: Create Account: Local Account, T1602.002: Data from Configuration Repository: Network Device Configuration Dump | <a href="https://mikrotik.com/supportsec/september-2026-vulnerability/">https://mikrotik.com/supportsec/september-2026-vulnerability/</a> |

| CVE ID                                            | CELEBRITY VULNERABILITY                                                           | AFFECTED PRODUCTS                                                                                                                       | ASSOCIATED ACTOR                                                                                                                                        |
|---------------------------------------------------|-----------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------|
| CVE-2026-65660                                    |  | Microsoft SharePoint Server Subscription Edition before 16.0.19725.20522, SharePoint Enterprise Server 2016, and SharePoint Server 2019 | -                                                                                                                                                       |
|                                                   | ZERO-DAY                                                                          |                                                                                                                                         |                                                                                                                                                         |
|                                                   |  | AFFECTED CPE                                                                                                                            | ASSOCIATED ATTACKS/RANSOMWARE                                                                                                                           |
| NAME                                              | BAS ATTACKS                                                                       | cpe:2.3:a:microsoft:sharepoint_server:*:*:*:*:*:*                                                                                       | -                                                                                                                                                       |
| Microsoft SharePoint Code Injection Vulnerability |  |                                                                                                                                         |                                                                                                                                                         |
|                                                   | CWE ID                                                                            | ASSOCIATED TTPs                                                                                                                         | PATCH LINK                                                                                                                                              |
|                                                   | CWE-94                                                                            | T1190: Exploit Public-Facing Application, T1059: Command and Scripting Interpreter                                                      | <a href="https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-65660">https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-65660</a> |

| CVE ID                                             | CELEBRITY VULNERABILITY                                                           | AFFECTED PRODUCTS                                                                                                                                                                                                      | ASSOCIATED ACTOR                                                                                                                                                                            |
|----------------------------------------------------|-----------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <u>CVE-2026-87902</u>                              |  | WordPress before 7.1.2, 7.0.6, 6.9.9, 6.8.10, 6.7.9, 6.6.9, 6.5.12, 6.4.12, 6.3.12, 6.2.13, 6.1.14, 6.0.16, 5.9.18, 5.8.17, 5.7.19, 5.6.21, 5.5.22, 5.4.23, 5.3.25, 5.2.28, 5.1.26, 5.0.29, 4.9.33, 4.8.32, and 4.7.37 | -                                                                                                                                                                                           |
|                                                    | ZERO-DAY                                                                          |                                                                                                                                                                                                                        |                                                                                                                                                                                             |
|                                                    |  | AFFECTED CPE                                                                                                                                                                                                           | ASSOCIATED ATTACKS/RANSOMWARE                                                                                                                                                               |
| NAME                                               | BAS ATTACKS                                                                       | cpe:2.3:a:wordpress:wordpress:*:*:*:*:*:*                                                                                                                                                                              | -                                                                                                                                                                                           |
| WordPress Core Remote File Inclusion Vulnerability |  |                                                                                                                                                                                                                        |                                                                                                                                                                                             |
|                                                    | CWE ID                                                                            | ASSOCIATED TTPs                                                                                                                                                                                                        | PATCH LINK                                                                                                                                                                                  |
|                                                    | CWE-98                                                                            | T1190: Exploit Public-Facing Application, T1059: Command and Scripting Interpreter                                                                                                                                     | <a href="https://github.com/WordPress/wordpress-develop/security/advisories/GHSA-7hp8-65ch-5whp">https://github.com/WordPress/wordpress-develop/security/advisories/GHSA-7hp8-65ch-5whp</a> |

| CVE ID                                              | CELEBRITY VULNERABILITY                                                            | AFFECTED PRODUCTS                                                                                                                                                                                                                                      | ASSOCIATED ACTOR                                                                                                                                                                                                                |
|-----------------------------------------------------|------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| CVE-2026-5430                                       |   | WSO2 API Manager before 4.6.0.21, 4.5.0.57, 4.4.0.72, 4.3.0.108, 4.2.0.197, and 4.1.0.257; WSO2 API Control Plane before 4.6.0.22 and 4.5.0.58; WSO2 Traffic Manager before 4.6.0.21 and 4.5.0.56; WSO2 Universal Gateway before 4.6.0.21 and 4.5.0.57 | -                                                                                                                                                                                                                               |
|                                                     | ZERO-DAY                                                                           |                                                                                                                                                                                                                                                        |                                                                                                                                                                                                                                 |
|                                                     |   | AFFECTED CPE                                                                                                                                                                                                                                           | ASSOCIATED ATTACKS/RANSOMWARE                                                                                                                                                                                                   |
| NAME                                                | BAS ATTACKS                                                                        | cpe:2.3:a:wso2:api_control_plane:*:*:*:*:*:*<br>cpe:2.3:a:wso2:api_manager:*:*:*:*:*:*<br>cpe:2.3:a:wso2:traffic_manager:*:*:*:*:*:*<br>cpe:2.3:a:wso2:universal_gateway:*:*:*:*:*:*                                                                   | -                                                                                                                                                                                                                               |
| WSO2 Multiple Products Path Traversal Vulnerability |  |                                                                                                                                                                                                                                                        |                                                                                                                                                                                                                                 |
|                                                     | CWE ID                                                                             | ASSOCIATED TTPs                                                                                                                                                                                                                                        | PATCH LINK                                                                                                                                                                                                                      |
|                                                     | CWE-347                                                                            | T1190: Exploit Public-Facing Application, T1606: Forge Web Credentials                                                                                                                                                                                 | <a href="https://security.docs.wso2.com/en/latest/security-announcements/security-advisories/2026/WSO2-2026-5328/">https://security.docs.wso2.com/en/latest/security-announcements/security-advisories/2026/WSO2-2026-5328/</a> |

| CVE ID                                                           | CELEBRITY VULNERABILITY                                                           | AFFECTED PRODUCTS                                                                                                                                                                                                                          | ASSOCIATED ACTOR                                                                                                                                |
|------------------------------------------------------------------|-----------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------|
| CVE-2026-71362                                                   |  | Adobe Commerce 2.4.9, 2.4.8-p5, 2.4.7-p10, 2.4.6-p15, 2.4.5-p17, 2.4.4-p18 and earlier; Adobe Commerce B2B 1.5.3, 1.5.2-p5, 1.4.2-p10, 1.3.4-p17, 1.3.3-p18 and earlier; Magento Open Source 2.4.9, 2.4.8-p5, 2.4.7-p10, 2.4.6 and earlier | -                                                                                                                                               |
|                                                                  | ZERO-DAY                                                                          |                                                                                                                                                                                                                                            |                                                                                                                                                 |
|                                                                  |  | AFFECTED CPE                                                                                                                                                                                                                               | ASSOCIATED ATTACKS/RANSOMWARE                                                                                                                   |
| NAME                                                             | BAS ATTACKS                                                                       | cpe:2.3:a:adobe:commerce:*:*:*:*:*<br>cpe:2.3:a:adobe:commerce_b2b:*:*:*:*:*<br>cpe:2.3:a:adobe:magento:*:*:*:*:*                                                                                                                          | -                                                                                                                                               |
| Adobe Commerce and Magento Incorrect Authorization Vulnerability |  |                                                                                                                                                                                                                                            |                                                                                                                                                 |
|                                                                  | CWE ID                                                                            | ASSOCIATED TTPs                                                                                                                                                                                                                            | PATCH LINK                                                                                                                                      |
|                                                                  | CWE-863                                                                           | T1190: Exploit Public-Facing Application, T1068: Exploitation for Privilege Escalation                                                                                                                                                     | <a href="https://helpx.adobe.com/security/products/magento/apsb26-92.html">https://helpx.adobe.com/security/products/magento/apsb26-92.html</a> |

| CVE ID                                                                | CELEBRITY VULNERABILITY                                                           | AFFECTED PRODUCTS                                                                                                                         | ASSOCIATED ACTOR                                                                                                                                                                                                      |
|-----------------------------------------------------------------------|-----------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <u>CVE-2026-93952</u>                                                 |  | Arista VeloCloud Orchestrator (on-premises) 5.2.0 before 5.2.3.16, 6.1.0 through 6.1.3.7, 6.4.0 before 6.4.2.8, and 7.0.0 through 7.0.0.2 | -                                                                                                                                                                                                                     |
|                                                                       | ZERO-DAY                                                                          |                                                                                                                                           |                                                                                                                                                                                                                       |
|                                                                       |  | AFFECTED CPE                                                                                                                              | ASSOCIATED ATTACKS/RANSOMWARE                                                                                                                                                                                         |
| NAME                                                                  | BAS ATTACKS                                                                       | cpe:2.3:a:arista:velocloud_orchestrator:*:*:*:*:*:*                                                                                       | -                                                                                                                                                                                                                     |
| Arista VeloCloud Orchestrator Improper Input Validation Vulnerability |  |                                                                                                                                           |                                                                                                                                                                                                                       |
|                                                                       | CWE ID                                                                            | ASSOCIATED TTPs                                                                                                                           | PATCH LINK                                                                                                                                                                                                            |
|                                                                       | CWE-20                                                                            | T1190: Exploit Public-Facing Application, T1059: Command and Scripting Interpreter                                                        | <a href="https://www.arista.com/en/support/advisories-notices/security-advisory/24765-security-advisory-0183">https://www.arista.com/en/support/advisories-notices/security-advisory/24765-security-advisory-0183</a> |

| CVE ID                                                 | CELEBRITY VULNERABILITY                                                           | AFFECTED PRODUCTS                                                                              | ASSOCIATED ACTOR                                                                                          |
|--------------------------------------------------------|-----------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------|
| <a href="#">CVE-2026-94127</a>                         |  | F5 BIG-IP Access Policy Manager (APM) 17.0.0 through 17.1.3, 17.5.0 through 17.5.1, and 21.1.0 | -                                                                                                         |
|                                                        | ZERO-DAY                                                                          |                                                                                                |                                                                                                           |
|                                                        |  | AFFECTED CPE                                                                                   | ASSOCIATED ATTACKS/RANSOMWARE                                                                             |
| NAME                                                   | BAS ATTACKS                                                                       | cpe:2.3:a:f5:big-ip_access_policy_manager:*:*:*:*:*                                            | -                                                                                                         |
| F5 BIG-IP APM Heap-based Buffer Overflow Vulnerability |  |                                                                                                |                                                                                                           |
|                                                        | CWE ID                                                                            | ASSOCIATED TTPs                                                                                | PATCH LINK                                                                                                |
|                                                        | CWE-122                                                                           | T1190: Exploit Public-Facing Application, T1059: Command and Scripting Interpreter             | <a href="https://my.f5.com/manage/s/article/K000162605">https://my.f5.com/manage/s/article/K000162605</a> |

| CVE ID                                                     | CELEBRITY VULNERABILITY                                                             | AFFECTED PRODUCTS                                                                                                             | ASSOCIATED ACTOR                                                                                                      |
|------------------------------------------------------------|-------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------|
| <a href="#">CVE-2026-93616</a>                             |  | Check Point Quantum Security Management and Multi-Domain Security Management R80 through R82.20                               | -                                                                                                                     |
|                                                            | ZERO-DAY                                                                            |                                                                                                                               |                                                                                                                       |
|                                                            |  | AFFECTED CPE                                                                                                                  | ASSOCIATED ATTACKS/RANSOMWARE                                                                                         |
| NAME                                                       | BAS ATTACKS                                                                         | cpe:2.3:a:checkpoint:multi-domain_security_management:*:*:*:*:*<br>cpe:2.3:a:checkpoint:quantum_security_management:*:*:*:*:* | -                                                                                                                     |
| Check Point Multiple Products Path Traversal Vulnerability |  |                                                                                                                               |                                                                                                                       |
|                                                            | CWE ID                                                                              | ASSOCIATED TTPs                                                                                                               | PATCH LINK                                                                                                            |
|                                                            | CWE-22                                                                              | T1190: Exploit Public-Facing Application                                                                                      | <a href="https://support.checkpoint.com/results/sk/sk1000171">https://support.checkpoint.com/results/sk/sk1000171</a> |

| CVE ID                                                                      | CELEBRITY VULNERABILITY                                                           | AFFECTED PRODUCTS                                                                                                                                 | ASSOCIATED ACTOR                                                                                                      |
|-----------------------------------------------------------------------------|-----------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------|
| <u>CVE-2026-85102</u>                                                       |  | Check Point Quantum Security Gateway on Gaia OS R80 through R82.10, and Gaia Embedded R81.10.00 through R81.10.17 and R82.00.00 through R82.00.10 | -                                                                                                                     |
|                                                                             | ZERO-DAY                                                                          |                                                                                                                                                   |                                                                                                                       |
|                                                                             |  | AFFECTED CPE                                                                                                                                      | ASSOCIATED ATTACKS/RANSOMWARE                                                                                         |
| NAME                                                                        | BAS ATTACKS                                                                       | cpe:2.3:o:checkpoint:gaia_embedded:*:*:*:*:*:*<br>cpe:2.3:o:checkpoint:gaia_os:*:*:*:*:*:*                                                        | -                                                                                                                     |
| Check Point Multiple Products Improper Certificate Validation Vulnerability |  |                                                                                                                                                   |                                                                                                                       |
|                                                                             | CWE ID                                                                            | ASSOCIATED TTPs                                                                                                                                   | PATCH LINK                                                                                                            |
|                                                                             | CWE-295                                                                           | T1190: Exploit Public-Facing Application, T1059: Command and Scripting Interpreter                                                                | <a href="https://support.checkpoint.com/results/sk/sk1000117">https://support.checkpoint.com/results/sk/sk1000117</a> |



| CVE ID                                    | CELEBRITY VULNERABILITY                                                           | AFFECTED PRODUCTS                                                                                                      | ASSOCIATED ACTOR                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
|-------------------------------------------|-----------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <u>CVE-2025-39964</u>                     |  | Linux kernel from 2.6.38 before 5.10.245, 5.15.194, 6.1.154, 6.6.108, 6.12.49, and 6.16.9, and 6.17 release candidates | -                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
|                                           | ZERO-DAY                                                                          |                                                                                                                        |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
|                                           |  | AFFECTED CPE                                                                                                           | ASSOCIATED ATTACKS/RANSOMWARE                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| NAME                                      | BAS ATTACKS                                                                       | cpe:2.3:o:linux:linux_kernel:*:*:*.*.*.*.*                                                                             | -                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| Linux Kernel Race Condition Vulnerability |  |                                                                                                                        |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
|                                           | CWE ID                                                                            | ASSOCIATED TTPs                                                                                                        | PATCH LINKS                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
|                                           | CWE-362                                                                           | T1068: Exploitation for Privilege Escalation                                                                           | <a href="https://git.kernel.org/stable/c/0f28c4adbc4a97437874c9b669fd7958a8c6d6ce">https://git.kernel.org/s<br/>table/c/0f28c4adbc4a<br/>97437874c9b669fd795<br/>8a8c6d6ce,</a><br><a href="https://git.kernel.org/sstable/c/1b34cbbf4f011a121ef7b2d7d6e6920a036d5285">https://git.kernel.org/s<br/>table/c/1b34cbbf4f011<br/>a121ef7b2d7d6e6920<br/>a036d5285,</a><br><a href="https://git.kernel.org/sstable/c/1f323a48e9b5ebfe6dc7d130fdf5c3c0e92a07c8">https://git.kernel.org/s<br/>table/c/1f323a48e9b5<br/>ebfe6dc7d130fdf5c3c0<br/>e92a07c8,</a><br><a href="https://git.kernel.org/sstable/c/45bcf60fe49b37daab1acee57b27211ad1574042">https://git.kernel.org/s<br/>table/c/45bcf60fe49b3<br/>7daab1acee57b27211<br/>ad1574042</a> |

| CVE ID                                         | CELEBRITY VULNERABILITY                                                           | AFFECTED PRODUCTS                                                                                                                                            | ASSOCIATED ACTOR                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
|------------------------------------------------|-----------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <u>CVE-2026-53266</u>                          |  | Linux kernel before 5.10.259, 5.15.210, 6.1.176, 6.6.143, 6.12.94, 6.18.36, and 7.0.13 (affected from 5.4.73, 5.8.17, and 5.9.2), and 7.1 release candidates | -                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
|                                                | ZERO-DAY                                                                          |                                                                                                                                                              |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
|                                                |  | AFFECTED CPE                                                                                                                                                 | ASSOCIATED ATTACKS/RANSOMWARE                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| NAME                                           | BAS ATTACKS                                                                       | cpe:2.3:o:linux:linux_kernel:*:*:*:*:*:*                                                                                                                     | -                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| Linux Kernel Out-of-Bounds Write Vulnerability |  |                                                                                                                                                              |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
|                                                | CWE ID                                                                            | ASSOCIATED TTPs                                                                                                                                              | PATCH LINKS                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
|                                                | CWE-787                                                                           | T1068: Exploitation for Privilege Escalation                                                                                                                 | <a href="https://git.kernel.org/s table/c/153ea96c806aea395daba907a4f88480b6ad5093">https://git.kernel.org/s table/c/153ea96c806aea395daba907a4f88480b6ad5093</a> ,<br><a href="https://git.kernel.org/s table/c/67ba971ae02514d85818fe0c32549ab4bfa3bf49">https://git.kernel.org/s table/c/67ba971ae02514d85818fe0c32549ab4bfa3bf49</a> ,<br><a href="https://git.kernel.org/s table/c/76280b78cc9f23bdc6438e10ad6dff148ef8375b">https://git.kernel.org/s table/c/76280b78cc9f23bdc6438e10ad6dff148ef8375b</a> ,<br><a href="https://git.kernel.org/s table/c/afd64b59c3de9bbbdd3759e834fdc55cda716e0b">https://git.kernel.org/s table/c/afd64b59c3de9bbbdd3759e834fdc55cda716e0b</a> |

| CVE ID                                                                          | CELEBRITY VULNERABILITY                                                           | AFFECTED PRODUCTS                                                                               | ASSOCIATED ACTOR                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
|---------------------------------------------------------------------------------|-----------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| CVE-2025-39682                                                                  |  | Linux kernel from 6.0 before 6.1.149, 6.6.103, 6.12.44, and 6.16.4, and 6.17 release candidates | -                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
|                                                                                 | ZERO-DAY                                                                          |                                                                                                 |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
|                                                                                 |  | AFFECTED CPE                                                                                    | ASSOCIATED ATTACKS/RANSOMWARE                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| NAME                                                                            | BAS ATTACKS                                                                       | cpe:2.3:o:linux:linux_kernel:*:*:*:*:*:*                                                        | -                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| Linux Kernel Improper Check for Unusual or Exceptional Conditions Vulnerability |  |                                                                                                 |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
|                                                                                 | CWE ID                                                                            | ASSOCIATED TTPs                                                                                 | PATCH LINKS                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
|                                                                                 | CWE-754                                                                           | T1068: Exploitation for Privilege Escalation                                                    | <a href="https://git.kernel.org/surface/c/2902c3ebcca52ca845c03182000e8d71d3a5196f">https://git.kernel.org/surface/c/2902c3ebcca52ca845c03182000e8d71d3a5196f</a> ,<br><a href="https://git.kernel.org/surface/c/29c0ce3c8cdb6dc5d61139c937f34cb888a6f42e">https://git.kernel.org/surface/c/29c0ce3c8cdb6dc5d61139c937f34cb888a6f42e</a> ,<br><a href="https://git.kernel.org/surface/c/3439c15ae91a517cf3c650ea15a8987699416ad9">https://git.kernel.org/surface/c/3439c15ae91a517cf3c650ea15a8987699416ad9</a> ,<br><a href="https://git.kernel.org/surface/c/62708b9452f8eb77513115b17c4f8d1a22ebf843">https://git.kernel.org/surface/c/62708b9452f8eb77513115b17c4f8d1a22ebf843</a> ,<br><a href="https://git.kernel.org/surface/c/c09dd3773b5950e9cfb6c9b9a5f6e36d06c62677">https://git.kernel.org/surface/c/c09dd3773b5950e9cfb6c9b9a5f6e36d06c62677</a> |

| CVE ID                                            | CELEBRITY VULNERABILITY                                                           | AFFECTED PRODUCTS                                                         | ASSOCIATED ACTOR                                                                                                                                              |
|---------------------------------------------------|-----------------------------------------------------------------------------------|---------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------|
| CVE-2026-58704                                    |  | Google Android (Cellular Modem component; NVD lists no specific versions) | -                                                                                                                                                             |
|                                                   | ZERO-DAY                                                                          |                                                                           |                                                                                                                                                               |
|                                                   |  | AFFECTED CPE                                                              | ASSOCIATED ATTACKS/RANSOMWARE                                                                                                                                 |
| NAME                                              | BAS ATTACKS                                                                       | cpe:2.3:o:google:android:*:*:*:*:*:*:*                                    | -                                                                                                                                                             |
| Google Pixel Improper Authorization Vulnerability |  |                                                                           |                                                                                                                                                               |
|                                                   | CWE ID                                                                            | ASSOCIATED TTPs                                                           | PATCH LINKS                                                                                                                                                   |
|                                                   | CWE-285                                                                           | T1404: Exploitation for Privilege Escalation (Mobile)                     | <a href="https://source.android.com/docs/security/bulletin/pixel/2026/2026-09-01">https://source.android.com/docs/security/bulletin/pixel/2026/2026-09-01</a> |



| CVE ID                                                     | CELEBRITY VULNERABILITY                                                           | AFFECTED PRODUCTS                                                                                                                                                                                                    | ASSOCIATED ACTOR                                                                                                                    |
|------------------------------------------------------------|-----------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------|
| <u>CVE-2026-87886</u>                                      |  | Acronis Backup plugin for cPanel & WHM (Linux) before build 1.9.3.1021, Acronis Backup extension for Plesk (Linux) before build 1.8.11.638, and Acronis Backup plugin for DirectAdmin (Linux) before build 1.2.3.238 | -                                                                                                                                   |
|                                                            | ZERO-DAY                                                                          |                                                                                                                                                                                                                      |                                                                                                                                     |
|                                                            |  | AFFECTED CPE                                                                                                                                                                                                         | ASSOCIATED ATTACKS/RANSOMWARE                                                                                                       |
| NAME                                                       | BAS ATTACKS                                                                       | cpe:2.3:a:acronis:acronis_backup:*:*:*:*:*:*                                                                                                                                                                         | -                                                                                                                                   |
| Acronis Backup Incorrect Default Permissions Vulnerability |  |                                                                                                                                                                                                                      |                                                                                                                                     |
|                                                            | CWE ID                                                                            | ASSOCIATED TTPs                                                                                                                                                                                                      | PATCH LINK                                                                                                                          |
|                                                            | CWE-276                                                                           | T1068: Exploitation for Privilege Escalation                                                                                                                                                                         | <a href="https://security-advisory.acronis.com/advisories/SEC-10986">https://security-advisory.acronis.com/advisories/SEC-10986</a> |

| CVE ID                                                 | CELEBRITY VULNERABILITY                                                           | AFFECTED PRODUCTS                                                                                                                                                                                                                                                               | ASSOCIATED ACTOR                                                                                                                                                                                                              |
|--------------------------------------------------------|-----------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <u>CVE-2026-76461</u>                                  |  | Cisco AsyncOS Software for Secure Email Gateway before 15.5.5-014, 16.0.4-302, and 16.5.0-780                                                                                                                                                                                   | -                                                                                                                                                                                                                             |
|                                                        | ZERO-DAY                                                                          |                                                                                                                                                                                                                                                                                 |                                                                                                                                                                                                                               |
|                                                        |  | AFFECTED CPE                                                                                                                                                                                                                                                                    | ASSOCIATED ATTACKS/RANSOMWARE                                                                                                                                                                                                 |
| NAME                                                   | BAS ATTACKS                                                                       | cpe:2.3:o:cisco:asyncos:*:*:*:*:*:*:*<br>cpe:2.3:a:cisco:secure_email_gateway_virtual_appliance_c100v:*:*:*:*:*:*:*<br>cpe:2.3:a:cisco:secure_email_gateway_virtual_appliance_c300v:*:*:*:*:*:*:*<br>cpe:2.3:a:cisco:secure_email_gateway_virtual_appliance_c600v:*:*:*:*:*:*:* | -                                                                                                                                                                                                                             |
| Cisco Secure Email Gateway SQL Injection Vulnerability |  |                                                                                                                                                                                                                                                                                 |                                                                                                                                                                                                                               |
|                                                        | CWE ID                                                                            | ASSOCIATED TTPs                                                                                                                                                                                                                                                                 | PATCH LINK                                                                                                                                                                                                                    |
|                                                        | CWE-89                                                                            | T1190: Exploit Public-Facing Application, T1059: Command and Scripting Interpreter                                                                                                                                                                                              | <a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-esa-inj-2bLVGmhX">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-esa-inj-2bLVGmhX</a> |

| CVE ID                                                                                          | CELEBRITY VULNERABILITY                                                           | AFFECTED PRODUCTS                                                                                                       | ASSOCIATED ACTOR                                                                                                                                                                                            |
|-------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <u>CVE-2026-84869</u>                                                                           |  | ConnectWise ScreenConnect client before 26.6.5.9742                                                                     | -                                                                                                                                                                                                           |
|                                                                                                 | ZERO-DAY                                                                          |                                                                                                                         |                                                                                                                                                                                                             |
|                                                                                                 |  | AFFECTED CPE                                                                                                            | ASSOCIATED ATTACKS/RANSOMWARE                                                                                                                                                                               |
| NAME                                                                                            | BAS ATTACKS                                                                       | cpe:2.3:a:connectwise:screenconnect:*:*:*:*:*:*                                                                         | -                                                                                                                                                                                                           |
| ConnectWise ScreenConnect Improper Privilege Management and Missing Authorization Vulnerability |  |                                                                                                                         |                                                                                                                                                                                                             |
|                                                                                                 | CWE ID                                                                            | ASSOCIATED TTPs                                                                                                         | PATCH LINK                                                                                                                                                                                                  |
|                                                                                                 | CWE-269                                                                           | T1219: Remote Access Software, T1059.005: Command and Scripting Interpreter: Visual Basic, T1570: Lateral Tool Transfer | <a href="https://www.connectwise.com/company/trust/security-bulletins/2026-09-08-screenconnect-bulletin">https://www.connectwise.com/company/trust/security-bulletins/2026-09-08-screenconnect-bulletin</a> |

| CVE ID                                                  | CELEBRITY VULNERABILITY                                                             | AFFECTED PRODUCTS                                                                      | ASSOCIATED ACTOR                                                                                                                            |
|---------------------------------------------------------|-------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------|
| <u>CVE-2026-42016</u>                                   |  | JFrog Artifactory (Self-Hosted) before 7.133.11                                        | -                                                                                                                                           |
|                                                         | ZERO-DAY                                                                            |                                                                                        |                                                                                                                                             |
|                                                         |  | AFFECTED CPE                                                                           | ASSOCIATED ATTACKS/RANSOMWARE                                                                                                               |
| NAME                                                    | BAS ATTACKS                                                                         | cpe:2.3:a:jfrog:artifactory:*:*:*:*:*:*                                                | -                                                                                                                                           |
| JFrog Artifactory Incorrect Authorization Vulnerability |  |                                                                                        |                                                                                                                                             |
|                                                         | CWE ID                                                                              | ASSOCIATED TTPs                                                                        | PATCH LINK                                                                                                                                  |
|                                                         | CWE-863                                                                             | T1190: Exploit Public-Facing Application, T1068: Exploitation for Privilege Escalation | <a href="https://docs.jfrog.com/releases/docs/jfrog-security-advisories">https://docs.jfrog.com/releases/docs/jfrog-security-advisories</a> |

| CVE ID                                                  | CELEBRITY VULNERABILITY                                                           | AFFECTED PRODUCTS                                                            | ASSOCIATED ACTOR                                                                                                                            |
|---------------------------------------------------------|-----------------------------------------------------------------------------------|------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------|
| <u>CVE-2026-42018</u>                                   |  | JFrog Artifactory before 7.111.20, 7.117.27, 7.125.19, 7.133.28, and 7.146.8 | -                                                                                                                                           |
|                                                         | ZERO-DAY                                                                          |                                                                              |                                                                                                                                             |
|                                                         |  | AFFECTED CPE                                                                 | ASSOCIATED ATTACKS/RANSOMWARE                                                                                                               |
| NAME                                                    | BAS ATTACKS                                                                       | cpe:2.3:a:jfrog:artifactory:*:*:*:*:*:*:*:*                                  | -                                                                                                                                           |
| JFrog Artifactory Improper Authentication Vulnerability |  |                                                                              |                                                                                                                                             |
|                                                         | CWE ID                                                                            | ASSOCIATED TTPs                                                              | PATCH LINK                                                                                                                                  |
|                                                         | CWE-287                                                                           | T1190: Exploit Public-Facing Application                                     | <a href="https://docs.jfrog.com/releases/docs/jfrog-security-advisories">https://docs.jfrog.com/releases/docs/jfrog-security-advisories</a> |

| CVE ID                                                                       | CELEBRITY VULNERABILITY                                                             | AFFECTED PRODUCTS                                                          | ASSOCIATED ACTOR                                                                                                                                                            |
|------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|----------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <u>CVE-2026-85706</u>                                                        |  | GitLab CE/EE from 18.7 before 18.11.12, 19.0.9, 19.1.8, 19.2.6, and 19.3.2 | -                                                                                                                                                                           |
|                                                                              | ZERO-DAY                                                                            |                                                                            |                                                                                                                                                                             |
|                                                                              |  | AFFECTED CPE                                                               | ASSOCIATED ATTACKS/RANSOMWARE                                                                                                                                               |
| NAME                                                                         | BAS ATTACKS                                                                         | cpe:2.3:a:gitlab:gitlab:*:*:*:*:*:*:*                                      | -                                                                                                                                                                           |
| GitLab Community Edition and Enterprise Edition Path Traversal Vulnerability |  |                                                                            |                                                                                                                                                                             |
|                                                                              | CWE ID                                                                              | ASSOCIATED TTPs                                                            | PATCH LINK                                                                                                                                                                  |
|                                                                              | CWE-22                                                                              | T1190: Exploit Public-Facing Application, T1005: Data from Local System    | <a href="https://docs.gitlab.com/releases/patches/patch-release-gitlab-19-3-2-released/">https://docs.gitlab.com/releases/patches/patch-release-gitlab-19-3-2-released/</a> |

| CVE ID                                                                                      | CELEBRITY VULNERABILITY                                                           | AFFECTED PRODUCTS                                                                                                                | ASSOCIATED ACTOR                                                                                                                          |
|---------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------|
| CVE-2026-86060                                                                              |  | MikroTik RouterOS before 6.49.21 (long-term), 7.23.4 (long-term), and 7.24.2 (stable)                                            | -                                                                                                                                         |
|                                                                                             | ZERO-DAY                                                                          |                                                                                                                                  |                                                                                                                                           |
|                                                                                             |  | AFFECTED CPE                                                                                                                     | ASSOCIATED ATTACKS/RANSOMWARE                                                                                                             |
| NAME                                                                                        | BAS ATTACKS                                                                       | cpe:2.3:o:mikrotik:routeros:*:*:*.*.*.*.*                                                                                        | -                                                                                                                                         |
| MikroTik RouterOS Improper Neutralization of Argument Delimiters in a Command Vulnerability |  |                                                                                                                                  |                                                                                                                                           |
|                                                                                             | CWE ID                                                                            | ASSOCIATED TTPs                                                                                                                  | PATCH LINK                                                                                                                                |
|                                                                                             | CWE-88                                                                            | T1190: Exploit Public-Facing Application, T1068: Exploitation for Privilege Escalation, T1136.001: Create Account: Local Account | <a href="https://mikrotik.com/supportsec/september-2026-vulnerability/">https://mikrotik.com/supportsec/september-2026-vulnerability/</a> |

| CVE ID                                                                       | CELEBRITY VULNERABILITY                                                           | AFFECTED PRODUCTS                                                                                                   | ASSOCIATED ACTOR                                                                                                                          |
|------------------------------------------------------------------------------|-----------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------|
| CVE-2026-67277                                                               |  | MikroTik RouterOS before 6.49.21 (long-term), 7.23.4 (long-term), and 7.24.2 (stable)                               | -                                                                                                                                         |
|                                                                              | ZERO-DAY                                                                          |                                                                                                                     |                                                                                                                                           |
|                                                                              |  | AFFECTED CPE                                                                                                        | ASSOCIATED ATTACKS/RANSOMWARE                                                                                                             |
| NAME                                                                         | BAS ATTACKS                                                                       | cpe:2.3:o:mikrotik:routeros:*:*:*.*.*.*.*.*                                                                         | -                                                                                                                                         |
| MikroTik RouterOS Missing Authentication for Critical Function Vulnerability |  |                                                                                                                     |                                                                                                                                           |
|                                                                              | CWE ID                                                                            | ASSOCIATED TTPs                                                                                                     | PATCH LINK                                                                                                                                |
|                                                                              | CWE-306                                                                           | T1190: Exploit Public-Facing Application, T1499.004: Endpoint Denial of Service: Application or System Exploitation | <a href="https://mikrotik.com/supportsec/september-2026-vulnerability/">https://mikrotik.com/supportsec/september-2026-vulnerability/</a> |

| CVE ID                                                                                  | CELEBRITY VULNERABILITY                                                           | AFFECTED PRODUCTS                                                                                                                                   | ASSOCIATED ACTOR                                                                                                                                                                |
|-----------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| CVE-2026-19490                                                                          |  | Citrix NetScaler ADC and NetScaler Gateway 14.1 through 14.1-73.32 and 13.1 through 13.1-63.21, and NetScaler ADC FIPS and NDcPP before 13.1-37.277 | -                                                                                                                                                                               |
|                                                                                         | ZERO-DAY                                                                          |                                                                                                                                                     |                                                                                                                                                                                 |
|                                                                                         |  | AFFECTED CPE                                                                                                                                        | ASSOCIATED ATTACKS/RANSOMWARE                                                                                                                                                   |
| NAME                                                                                    | BAS ATTACKS                                                                       | cpe:2.3:a:citrix:netcaler_application_delivery_controller:*:*:*:*:*:*<br>cpe:2.3:a:citrix:netcaler_gateway:*:*:*:*:*:*                              | -                                                                                                                                                                               |
| Citrix NetScaler Authentication Bypass Using an Alternate Path or Channel Vulnerability |  |                                                                                                                                                     |                                                                                                                                                                                 |
|                                                                                         | CWE ID                                                                            | ASSOCIATED TTPs                                                                                                                                     | PATCH LINK                                                                                                                                                                      |
|                                                                                         | CWE-288                                                                           | T1190: Exploit Public-Facing Application, T1133: External Remote Services                                                                           | <a href="https://support.citrix.com/support-home/kbsearch/article?articleNumber=CTX696939">https://support.citrix.com/support-home/kbsearch/article?articleNumber=CTX696939</a> |

| CVE ID                                                              | CELEBRITY VULNERABILITY                                                           | AFFECTED PRODUCTS                                                                                                                                                                                                          | ASSOCIATED ACTOR                                                                                                    |
|---------------------------------------------------------------------|-----------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------|
| CVE-2025-25249                                                      |  | Fortinet FortiOS 6.4 all versions, 7.0.0 through 7.0.17, 7.2.0 through 7.2.11, 7.4.0 through 7.4.8, and 7.6.0 through 7.6.3; FortiSwitchManager 7.0.0 through 7.0.5 and 7.2.0 through 7.2.6; FortiSASE 25.1.39 and 25.1.51 | -                                                                                                                   |
|                                                                     | ZERO-DAY                                                                          |                                                                                                                                                                                                                            |                                                                                                                     |
|                                                                     |  | AFFECTED CPE                                                                                                                                                                                                               | ASSOCIATED ATTACKS/RANSOMWARE                                                                                       |
| NAME                                                                | BAS ATTACKS                                                                       | cpe:2.3:o:fortinet:fortios:*:*:*:*:*:*<br>cpe:2.3:a:fortinet:fortiswitchmanager:*:*:*:*:*:*<br>cpe:2.3:a:fortinet:fortisase:*:*:*:*:*:*                                                                                    | -                                                                                                                   |
| Fortinet Multiple Products Heap-based Buffer Overflow Vulnerability |  |                                                                                                                                                                                                                            |                                                                                                                     |
|                                                                     | CWE ID                                                                            | ASSOCIATED TTPs                                                                                                                                                                                                            | PATCH LINK                                                                                                          |
|                                                                     | CWE-122                                                                           | T1190: Exploit Public-Facing Application, T1552.001: Unsecured Credentials: Credentials In Files, T1090: Proxy                                                                                                             | <a href="https://fortiguard.fortinet.com/psirt/FG-IR-25-084">https://fortiguard.fortinet.com/psirt/FG-IR-25-084</a> |

| CVE ID                                               | CELEBRITY VULNERABILITY                                                           | AFFECTED PRODUCTS                                                                                                          | ASSOCIATED ACTOR                                                                                                                                                                                            |
|------------------------------------------------------|-----------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <u>CVE-2026-87491</u>                                |  | Google Chrome before 153.0.8010.36                                                                                         | APT31 (TA412 / JungleBamboo), UTA0560, UTA0565, UNK_LateNight, UNK_DoubleCheck, UNK_QuietRacket                                                                                                             |
|                                                      | ZERO-DAY                                                                          |                                                                                                                            |                                                                                                                                                                                                             |
|                                                      |  | AFFECTED CPE                                                                                                               | ASSOCIATED ATTACKS/RANSOMWARE                                                                                                                                                                               |
| NAME                                                 | BAS ATTACKS                                                                       | cpe:2.3:a:google:chrome:*:*:*:*:*:*:*:*                                                                                    | GemStone (LONGTALE) SUPERSTOMP GRIMWEDGE CLEANGULP ShadowPad                                                                                                                                                |
| Google Chromium V8 Out of Bounds Write Vulnerability |  |                                                                                                                            |                                                                                                                                                                                                             |
|                                                      | CWE ID                                                                            | ASSOCIATED TTPs                                                                                                            | PATCH LINK                                                                                                                                                                                                  |
|                                                      | CWE-787                                                                           | T1566.002: Phishing: Spearphishing Link, T1203: Exploitation for Client Execution, T1211: Exploitation for Defense Evasion | <a href="https://chromerelease.googleblog.com/2026/09/stable-channel-update-for-desktop_0808145027.html">https://chromerelease.googleblog.com/2026/09/stable-channel-update-for-desktop_0808145027.html</a> |

| CVE ID                                                                                                  | CELEBRITY VULNERABILITY                                                           | AFFECTED PRODUCTS                                                                                                                                   | ASSOCIATED ACTOR                                                                                                                                                                                                                                          |
|---------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| CVE-2026-20079                                                                                          |  | Cisco Secure Firewall Management Center (FMC) Software 7.0, 7.1, 7.2, 7.3, 7.4, 7.6, 7.7, and 10.0                                                  | UAT-11823, UAT-12197                                                                                                                                                                                                                                      |
|                                                                                                         | ZERO-DAY                                                                          |                                                                                                                                                     |                                                                                                                                                                                                                                                           |
|                                                                                                         |  | AFFECTED CPE                                                                                                                                        | ASSOCIATED ATTACKS/RANSOMWARE                                                                                                                                                                                                                             |
| NAME                                                                                                    | BAS ATTACKS                                                                       | cpe:2.3:a:cisco:secure_firewall_management_center:*:*:*:*:*:*:*                                                                                     | Cyclops Blink JSP web shell cmd.jar                                                                                                                                                                                                                       |
| Cisco Firewall Management Center Authentication Bypass Using an Alternate Path or Channel Vulnerability |  |                                                                                                                                                     |                                                                                                                                                                                                                                                           |
|                                                                                                         | CWE ID                                                                            | ASSOCIATED TTPs                                                                                                                                     | PATCH LINK                                                                                                                                                                                                                                                |
|                                                                                                         | CWE-288                                                                           | T1190: Exploit Public-Facing Application, T1505.003: Server Software Component: Web Shell, T1059.004: Command and Scripting Interpreter: Unix Shell | <a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-onprem-fmc-authbypass-5JPp45V2">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-onprem-fmc-authbypass-5JPp45V2</a> |

| CVE ID                                                                                                         | CELEBRITY VULNERABILITY                                                           | AFFECTED PRODUCTS                                                                                                                                                                                                                              | ASSOCIATED ACTOR                                                                                                                                  |
|----------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------|
| <b><u>CVE-2026-75650</u></b>                                                                                   | StyleSmuggler                                                                     | Adobe Commerce 2.4.9, 2.4.8-p5, 2.4.7-p10, 2.4.6-p15, 2.4.5-p17, 2.4.4-p18 and earlier; Adobe Commerce B2B 1.5.3, 1.5.2-p5, 1.4.2-p10, 1.3.4-p17, 1.3.3-p18 and earlier; Magento Open Source 2.4.9, 2.4.8-p5, 2.4.7-p10, 2.4.6-p15 and earlier | -                                                                                                                                                 |
|                                                                                                                | <b>ZERO-DAY</b>                                                                   |                                                                                                                                                                                                                                                |                                                                                                                                                   |
|                                                                                                                |  | <b>AFFECTED CPE</b>                                                                                                                                                                                                                            | <b>ASSOCIATED ATTACKS/RANSOMWARE</b>                                                                                                              |
| <b>NAME</b>                                                                                                    | <b>BAS ATTACKS</b>                                                                | cpe:2.3:a:adobe:commerce:*:*:*:*:*<br>cpe:2.3:a:adobe:commerce_b2b:*:*:*:*:*<br>cpe:2.3:a:adobe:magento:*:*:*:*:*                                                                                                                              | -                                                                                                                                                 |
| Adobe Commerce and Magento Improper Neutralization of Special Elements Used in a Template Engine Vulnerability |  |                                                                                                                                                                                                                                                |                                                                                                                                                   |
|                                                                                                                | <b>CWE ID</b>                                                                     | <b>ASSOCIATED TTPs</b>                                                                                                                                                                                                                         | <b>PATCH LINK</b>                                                                                                                                 |
|                                                                                                                | CWE-1336                                                                          | T1190: Exploit Public-Facing Application, T1059: Command and Scripting Interpreter                                                                                                                                                             | <a href="https://helpx.adobe.com/security/products/magento/apsb26-146.html">https://helpx.adobe.com/security/products/magento/apsb26-146.html</a> |

| CVE ID                                         | CELEBRITY VULNERABILITY                                                            | AFFECTED PRODUCTS                                                                                                                                                                                                                                               | ASSOCIATED ACTOR                                                                                                                                        |
|------------------------------------------------|------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------|
| <u>CVE-2026-81963</u>                          |   | Microsoft Windows 11 23H2 before 10.0.22631.7582, 24H2 before 10.0.26100.9445, 25H2 before 10.0.26200.9445, and 26H1 before 10.0.28000.2954; Windows Server 2025 before 10.0.26100.33438                                                                        | -                                                                                                                                                       |
|                                                | ZERO-DAY                                                                           |                                                                                                                                                                                                                                                                 |                                                                                                                                                         |
|                                                |   | AFFECTED CPE                                                                                                                                                                                                                                                    | ASSOCIATED ATTACKS/RANSOMWARE                                                                                                                           |
| NAME                                           | BAS ATTACKS                                                                        | cpe:2.3:o:microsoft:windows_11_23h2:*:*:*:*:*:*<br>cpe:2.3:o:microsoft:windows_11_24h2:*:*:*:*:*:*<br>cpe:2.3:o:microsoft:windows_11_25h2:*:*:*:*:*:*<br>cpe:2.3:o:microsoft:windows_11_26h1:*:*:*:*:*:*<br>cpe:2.3:o:microsoft:windows_server_2025:*:*:*:*:*:* | -                                                                                                                                                       |
| Microsoft Windows Link Following Vulnerability |  |                                                                                                                                                                                                                                                                 |                                                                                                                                                         |
|                                                | CWE ID                                                                             | ASSOCIATED TTPs                                                                                                                                                                                                                                                 | PATCH LINK                                                                                                                                              |
|                                                | CWE-59                                                                             | T1068: Exploitation for Privilege Escalation                                                                                                                                                                                                                    | <a href="https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-81963">https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-81963</a> |

| CVE ID                                               | CELEBRITY VULNERABILITY                                                           | AFFECTED PRODUCTS                                                                  | ASSOCIATED ACTOR                                                                                                                                                                                                                                  |
|------------------------------------------------------|-----------------------------------------------------------------------------------|------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <u>CVE-2026-86218</u>                                |  | N-able N-central before 2026.3.1.14                                                | -                                                                                                                                                                                                                                                 |
|                                                      | ZERO-DAY                                                                          |                                                                                    |                                                                                                                                                                                                                                                   |
|                                                      |  | AFFECTED CPE                                                                       | ASSOCIATED ATTACKS/RANSOMWARE                                                                                                                                                                                                                     |
| NAME                                                 | BAS ATTACKS                                                                       | cpe:2.3:a:n-able:n-central:*:*:*:*:*:*                                             | -                                                                                                                                                                                                                                                 |
| N-able N-central Static Code Injection Vulnerability |  |                                                                                    |                                                                                                                                                                                                                                                   |
|                                                      | CWE ID                                                                            | ASSOCIATED TTPs                                                                    | PATCH LINK                                                                                                                                                                                                                                        |
|                                                      | CWE-96                                                                            | T1190: Exploit Public-Facing Application, T1059: Command and Scripting Interpreter | <a href="https://me.n-able.com/s/security-advisory/aArVy0000002Ld3KAE/cve202686218-preauthentication-remote-code-execution">https://me.n-able.com/s/security-advisory/aArVy0000002Ld3KAE/cve202686218-preauthentication-remote-code-execution</a> |

| CVE ID                                                     | CELEBRITY VULNERABILITY                                                             | AFFECTED PRODUCTS                                                                                                                                                                                                                                                                                                                                                                                                                    | ASSOCIATED ACTOR                                                                                                                                        |
|------------------------------------------------------------|-------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------|
| <u>CVE-2026-85880</u>                                      |    | Microsoft Windows 10 1607 before 10.0.14393.9512, 1809 before 10.0.17763.9245, 21H2 before 10.0.19044.7725, and 22H2 before 10.0.19045.7725; Windows Server 2012 and 2012 R2; Windows Server 2016 before 10.0.14393.9512, 2019 before 10.0.17763.9245, and 2022 before 10.0.20348.5622                                                                                                                                               | APT31 (TA412 / JungleBamboo), UTA0560, UTA0565, UNK_LateNight, UNK_DoubleCheck, UNK_QuietRacket                                                         |
|                                                            | ZERO-DAY                                                                            |                                                                                                                                                                                                                                                                                                                                                                                                                                      |                                                                                                                                                         |
|                                                            |    | AFFECTED CPE                                                                                                                                                                                                                                                                                                                                                                                                                         | ASSOCIATED ATTACKS/RANSOMWARE                                                                                                                           |
| NAME                                                       | BAS ATTACKS                                                                         | cpe:2.3:o:microsoft:windows_10_1607:*:*:*:*:*:*<br>cpe:2.3:o:microsoft:windows_10_1809:*:*:*:*:*:*<br>cpe:2.3:o:microsoft:windows_10_21h2:*:*:*:*:*:*<br>cpe:2.3:o:microsoft:windows_10_22h2:*:*:*:*:*:*<br>cpe:2.3:o:microsoft:windows_server_2012:*:*:*:*:*:*<br>cpe:2.3:o:microsoft:windows_server_2016:*:*:*:*:*:*<br>cpe:2.3:o:microsoft:windows_server_2019:*:*:*:*:*:*<br>cpe:2.3:o:microsoft:windows_server_2022:*:*:*:*:*:* | GemStone (LONGTALE)<br>SUPERSTOMP<br>GRIMWEDGE<br>CLEANGULP<br>ShadowPad                                                                                |
| Microsoft Windows Heap-Based Buffer Overflow Vulnerability |  |                                                                                                                                                                                                                                                                                                                                                                                                                                      |                                                                                                                                                         |
|                                                            | CWE ID                                                                              | ASSOCIATED TTPs                                                                                                                                                                                                                                                                                                                                                                                                                      | PATCH LINK                                                                                                                                              |
|                                                            | CWE-122                                                                             | T1068: Exploitation for Privilege Escalation, T1055: Process Injection, T1176.001: Software Extensions: Browser Extensions                                                                                                                                                                                                                                                                                                           | <a href="https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-85880">https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-85880</a> |

| CVE ID                                          | CELEBRITY VULNERABILITY                                                           | AFFECTED PRODUCTS                                                                                                                           | ASSOCIATED ACTOR                                                                                                                                                                                                  |
|-------------------------------------------------|-----------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <u>CVE-2026-85046</u>                           |  | Google Chrome before 152.0.7977.82                                                                                                          | APT31 (TA412 / JungleBamboo), UTA0560, UTA0565, UNK_LateNight, UNK_DoubleCheck, UNK_QuietRacket                                                                                                                   |
|                                                 | ZERO-DAY                                                                          |                                                                                                                                             |                                                                                                                                                                                                                   |
|                                                 |  | AFFECTED CPE                                                                                                                                | ASSOCIATED ATTACKS/RANSOMWARE                                                                                                                                                                                     |
| NAME                                            | BAS ATTACKS                                                                       | cpe:2.3:a:google:chrome:*:*:*:*:*:*:*:*:*:*<br>cpe:2.3:a:google:v8:*:*:*:*:*:*:*:*                                                          | GemStone (LONGTALE) SUPERSTOMP GRIMWEDGE CLEANGULP ShadowPad                                                                                                                                                      |
| Google Chromium V8 Type Confusion Vulnerability |  |                                                                                                                                             |                                                                                                                                                                                                                   |
|                                                 | CWE ID                                                                            | ASSOCIATED TTPs                                                                                                                             | PATCH LINK                                                                                                                                                                                                        |
|                                                 | CWE-843                                                                           | T1566.002: Phishing: Spearphishing Link, T1203: Exploitation for Client Execution, T1059.007: Command and Scripting Interpreter: JavaScript | <a href="https://chromerelease.s.googleblog.com/2026/09/stable-channel-update-for-desktop_01882797386.html">https://chromerelease.s.googleblog.com/2026/09/stable-channel-update-for-desktop_01882797386.html</a> |

| CVE ID                                                | CELEBRITY VULNERABILITY                                                           | AFFECTED PRODUCTS                         | ASSOCIATED ACTOR                                                                                                                                                    |
|-------------------------------------------------------|-----------------------------------------------------------------------------------|-------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| CVE-2026-59822                                        |  | LiteLLM before 1.84.0                     | -                                                                                                                                                                   |
|                                                       | ZERO-DAY                                                                          |                                           |                                                                                                                                                                     |
|                                                       |  | AFFECTED CPE                              | ASSOCIATED ATTACKS/RANSOMWARE                                                                                                                                       |
| NAME                                                  | BAS ATTACKS                                                                       | cpe:2.3:a:litellm:litellm:*.*.*.*:*.*.*.* | -                                                                                                                                                                   |
| BerriAI LiteLLM Improper Authentication Vulnerability |  |                                           |                                                                                                                                                                     |
|                                                       | CWE ID                                                                            | ASSOCIATED TTPs                           | PATCH LINK                                                                                                                                                          |
|                                                       | CWE-287                                                                           | T1190: Exploit Public-Facing Application  | <a href="https://github.com/BerriAI/litellm/security/advisories/GHSA-7488-6r32-c95q">https://github.com/BerriAI/litellm/security/advisories/GHSA-7488-6r32-c95q</a> |

| CVE ID                                                         | CELEBRITY VULNERABILITY                                                           | AFFECTED PRODUCTS                                                                                                                                | ASSOCIATED ACTOR                                                                                                                                                      |
|----------------------------------------------------------------|-----------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <u>CVE-2026-48710</u>                                          | BadHost                                                                           | Starlette from 0.8.3 before 1.0.1                                                                                                                | -                                                                                                                                                                     |
|                                                                | ZERO-DAY                                                                          |                                                                                                                                                  |                                                                                                                                                                       |
|                                                                |  | AFFECTED CPE                                                                                                                                     | ASSOCIATED ATTACKS/RANSOMWARE                                                                                                                                         |
| NAME                                                           | BAS ATTACKS                                                                       | cpe:2.3:a:encode:starlette:*:*:*:*:*:*:*:*:*:*                                                                                                   | XMRig                                                                                                                                                                 |
| Kludex Starlette HTTP Request/Response Smuggling Vulnerability |  |                                                                                                                                                  |                                                                                                                                                                       |
|                                                                | CWE ID                                                                            | ASSOCIATED TTPs                                                                                                                                  | PATCH LINK                                                                                                                                                            |
|                                                                | CWE-444                                                                           | T1190: Exploit Public-Facing Application, T1496.001: Resource Hijacking: Compute Hijacking, T1098.004: Account Manipulation: SSH Authorized Keys | <a href="https://github.com/Kludex/starlette/security/advisories/GHSA-86qp-5c8j-p5mr">https://github.com/Kludex/starlette/security/advisories/GHSA-86qp-5c8j-p5mr</a> |

| CVE ID                                        | CELEBRITY VULNERABILITY                                                           | AFFECTED PRODUCTS                                                                                                                   | ASSOCIATED ACTOR                                                                                                                                                      |
|-----------------------------------------------|-----------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| CVE-2026-49869                                |  | Kestra OSS before 1.0.45 and 1.3.21                                                                                                 | -                                                                                                                                                                     |
|                                               | ZERO-DAY                                                                          |                                                                                                                                     |                                                                                                                                                                       |
|                                               |  | AFFECTED CPE                                                                                                                        | ASSOCIATED ATTACKS/RANSOMWARE                                                                                                                                         |
| NAME                                          | BAS ATTACKS                                                                       | cpe:2.3:a:kestra:kestra:*:*:*:*:*:*:*                                                                                               | XMRig                                                                                                                                                                 |
| Kestra OSS OS Command Injection Vulnerability |  |                                                                                                                                     |                                                                                                                                                                       |
|                                               | CWE ID                                                                            | ASSOCIATED TTPs                                                                                                                     | PATCH LINK                                                                                                                                                            |
|                                               | CWE-78                                                                            | T1190: Exploit Public-Facing Application, T1613: Container and Resource Discovery, T1496.001: Resource Hijacking: Compute Hijacking | <a href="https://github.com/kestra-io/kestra/security/advisories/GHSA-5vc5-wxxq-3fjx">https://github.com/kestra-io/kestra/security/advisories/GHSA-5vc5-wxxq-3fjx</a> |

| CVE ID                                                  | CELEBRITY VULNERABILITY                                                           | AFFECTED PRODUCTS                                                                                    | ASSOCIATED ACTOR                                                                                                                            |
|---------------------------------------------------------|-----------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------|
| <u>CVE-2026-82329</u>                                   |  | JFrog Artifactory from 7.111.4 before 7.111.21, 7.117.28, 7.125.20, 7.133.29, 7.146.38, and 7.161.20 | -                                                                                                                                           |
|                                                         | ZERO-DAY                                                                          |                                                                                                      |                                                                                                                                             |
|                                                         |  | AFFECTED CPE                                                                                         | ASSOCIATED ATTACKS/RANSOMWARE                                                                                                               |
| NAME                                                    | BAS ATTACKS                                                                       | cpe:2.3:a:jfrog:artifactory:*:*:*:*:*:*:*:*                                                          | -                                                                                                                                           |
| JFrog Artifactory Improper Authentication Vulnerability |  |                                                                                                      |                                                                                                                                             |
|                                                         | CWE ID                                                                            | ASSOCIATED TTPs                                                                                      | PATCH LINK                                                                                                                                  |
|                                                         | CWE-287                                                                           | T1190: Exploit Public-Facing Application                                                             | <a href="https://docs.jfrog.com/releases/docs/jfrog-security-advisories">https://docs.jfrog.com/releases/docs/jfrog-security-advisories</a> |

| CVE ID                                        | CELEBRITY VULNERABILITY                                                           | AFFECTED PRODUCTS                                                                  | ASSOCIATED ACTOR                                                                                                                                                                                                                                                          |
|-----------------------------------------------|-----------------------------------------------------------------------------------|------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| CVE-2026-9586                                 |  | Sangoma Switchvox from 8.2.2.1 before 8.4.0.2                                      | -                                                                                                                                                                                                                                                                         |
|                                               | ZERO-DAY                                                                          |                                                                                    |                                                                                                                                                                                                                                                                           |
|                                               |  | AFFECTED CPE                                                                       | ASSOCIATED ATTACKS/RANSOMWARE                                                                                                                                                                                                                                             |
| NAME                                          | BAS ATTACKS                                                                       | cpe:2.3:a:sangoma:switchvox:*:*:*:*:*:*                                            | -                                                                                                                                                                                                                                                                         |
| Sangoma Switchvox SQL Injection Vulnerability |  |                                                                                    |                                                                                                                                                                                                                                                                           |
|                                               | CWE ID                                                                            | ASSOCIATED TTPs                                                                    | PATCH LINK                                                                                                                                                                                                                                                                |
|                                               | CWE-89                                                                            | T1190: Exploit Public-Facing Application, T1059: Command and Scripting Interpreter | <a href="https://sangomakb.atlassian.net/wiki/spaces/Switchvox/pages/1802371073/Switchvox+-+Release+Notes+Version+8.4.0.2+July+14+2026">https://sangomakb.atlassian.net/wiki/spaces/Switchvox/pages/1802371073/Switchvox+-+Release+Notes+Version+8.4.0.2+July+14+2026</a> |

| CVE ID                                                                 | CELEBRITY VULNERABILITY                                                           | AFFECTED PRODUCTS                                                                                                                                | ASSOCIATED ACTOR                                                                                                                              |
|------------------------------------------------------------------------|-----------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------|
| <u>CVE-2026-83548</u>                                                  |  | SonicWall SMA1000 series (SMA 6210, SMA 7210, and SMA 8200v) before 12.4.3-03526 and 12.5.0-02952                                                | -                                                                                                                                             |
|                                                                        | ZERO-DAY                                                                          |                                                                                                                                                  |                                                                                                                                               |
|                                                                        |  | AFFECTED CPE                                                                                                                                     | ASSOCIATED ATTACKS/RANSOMWARE                                                                                                                 |
| NAME                                                                   | BAS ATTACKS                                                                       | cpe:2.3:a:sonicwall:sma8200v:*:*:*:*:*:*<br>cpe:2.3:o:sonicwall:sma6210_firmware:*:*:*:*:*:*<br>cpe:2.3:o:sonicwall:sma7210_firmware:*:*:*:*:*:* | -                                                                                                                                             |
| SonicWall SMA1000 Appliances Server-Side Request Forgery Vulnerability |  |                                                                                                                                                  |                                                                                                                                               |
|                                                                        | CWE ID                                                                            | ASSOCIATED TTPs                                                                                                                                  | PATCH LINK                                                                                                                                    |
|                                                                        | CWE-441                                                                           | T1190: Exploit Public-Facing Application, T1090: Proxy                                                                                           | <a href="https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2026-0016">https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2026-0016</a> |

| CVE ID                                                          | CELEBRITY VULNERABILITY                                                           | AFFECTED PRODUCTS                                                                                                                                | ASSOCIATED ACTOR                                                                                                                              |
|-----------------------------------------------------------------|-----------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------|
| <u>CVE-2026-83549</u>                                           |  | SonicWall SMA1000 series (SMA 6210, SMA 7210, and SMA 8200v) before 12.4.3-03526 and 12.5.0-02952                                                | -                                                                                                                                             |
|                                                                 | ZERO-DAY                                                                          |                                                                                                                                                  |                                                                                                                                               |
|                                                                 |  | AFFECTED CPE                                                                                                                                     | ASSOCIATED ATTACKS/RANSOMWARE                                                                                                                 |
| NAME                                                            | BAS ATTACKS                                                                       | cpe:2.3:a:sonicwall:sma8200v:*:*:*:*:*:*<br>cpe:2.3:o:sonicwall:sma6210_firmware:*:*:*:*:*:*<br>cpe:2.3:o:sonicwall:sma7210_firmware:*:*:*:*:*:* | -                                                                                                                                             |
| SonicWall SMA1000 Appliances OS Command Injection Vulnerability |  |                                                                                                                                                  |                                                                                                                                               |
|                                                                 | CWE ID                                                                            | ASSOCIATED TTPs                                                                                                                                  | PATCH LINK                                                                                                                                    |
|                                                                 | CWE-78                                                                            | T1190: Exploit Public-Facing Application, T1059: Command and Scripting Interpreter                                                               | <a href="https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2026-0016">https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2026-0016</a> |

# Recommendations

- ☼ To ensure the security of their systems and data, organizations should prioritize the vulnerabilities listed above and promptly apply patches to them before the due date provided.
- ☼ It is essential to comply with BINDING OPERATIONAL DIRECTIVE 26-04 provided by the Cyber security and Infrastructure Security Agency (CISA). This directive outlines the minimum cybersecurity standards that all federal agencies must follow to protect their organization from cybersecurity threats.
- ☼ The affected products listed in the report can help organizations identify assets that have been affected by KEVs, even without conducting a scan. These assets should be patched with priority to reduce the risk.

# References

<https://www.cisa.gov/known-exploited-vulnerabilities-catalog>

## Appendix

**Celebrity Vulnerabilities:** Software vulnerabilities that have gained significant attention and have been branded with catchy names and logos due to their profound and multifaceted impact. These vulnerabilities provide threat actors with opportunities to breach sensitive systems, potentially resulting in unauthorized access and the compromise of critical information.

**BAS Attacks:** “BAS attacks” are the simulated cyber-attacks that can be carried out by our in-house Uni5's Breach and Attack Simulation (BAS), which organizations could use to identify vulnerabilities and improve their overall security posture.

**Due Date:** The "Due Date" provided by CISA is a recommended deadline that organizations should use to prioritize the remediation of identified vulnerabilities in their systems, with the aim of enhancing their overall security posture.

# What Next?

At Hive Pro, it is our mission to detect the most likely threats to your organization and to help you prevent them from happening.

Book a Demo of HivePro.

REPORT GENERATED ON

**October 05, 2026 • 10:30 AM**

© 2026 All Rights are Reserved by Hive Pro



More at [www.hivepro.com](http://www.hivepro.com)