Date of Publication
November 05, 2026

Hive Pro

Hiveforce Labs

CISA KNOWN EXPLOITED VULNERABILITY CATALOG

October 2026

Table of Contents

Summary 03

CVEs List 04

CVEs Details 12

Recommendations 46

References 47

Appendix 47

What Next? 48

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 **October 2026**, **36** vulnerabilities met the criteria for inclusion in the CISA's KEV catalog. Of these, **18** are **zero-day** vulnerabilities; **19** have been **exploited** by a threat actor and employed in attacks.

36
Known Exploited Vulnerabilities



CVEs List

CVE	NAME	AFFECTED PRODUCT	CVSS 3.x SCORE	ZERO-DAY	PATCH	DUE DATE
CVE-2026-118527	Ivanti Connect Secure Generation of Predictable Numbers or Identifiers Vulnerability	Ivanti Connect Secure	4.3	✓	✓	November 13, 2026
CVE-2026-111357	Ivanti Connect Secure Missing Authentication for Critical Function Vulnerability	Ivanti Connect Secure	7	✓	✓	November 02, 2026
CVE-2026-97229	GitLab Community Edition and Enterprise Edition Integer Overflow or Wraparound Vulnerability	GitLab Community Edition and Enterprise Edition	10	✗	✓	November 01, 2026

CVE	NAME	AFFECTED PRODUCT	CVSS 3.x SCORE	ZERO-DAY	PATCH	DUE DATE
CVE-2026-76418	Cisco Secure Firewall ASA Software and Cisco Secure FTD Software Unchecked Return Value to NULL Pointer Dereference Vulnerability	Cisco Secure Firewall ASA Software and Cisco Secure FTD Software	8.6			November 01, 2026
CVE-2026-41709	Broadcom VMWare ESX Insufficient Logging Vulnerability	Broadcom VMware ESX	2.7			November 11, 2026
CVE-2026-46300	Linux Kernel Missing Initialization of a Variable Vulnerability	Linux Kernel	7.8			October 31, 2026
CVE-2026-48356	Adobe Commerce and Magento Unrestricted Upload of File with Dangerous Type Vulnerability	Adobe Commerce and Magento	9.3			November 10, 2026
CVE-2026-111497	Google Brotli Unchecked Return Value Vulnerability	Google Brotli	9.8			November 10, 2026

CVE	NAME	AFFECTED PRODUCT	CVSS 3.x SCORE	ZERO-DAY	PATCH	DUE DATE
CVE-2026-109618	PHP Memory Corruption Vulnerability	PHP Group	9.8	✗	✓	October 29, 2026
CVE-2026-109619	PHP Stale Internal Request-State Vulnerability	PHP Group	8.1	✗	✓	October 29, 2026
CVE-2026-114625	Arista VeloCloud Orchestrator SQL Injection Vulnerability	Arista VeloCloud Orchestrator	9.9	✓	✓	October 26, 2026
CVE-2026-110447	Collabora Online – Built-in CODE Server OS Command Injection Vulnerability	Collabora Online – Built-in CODE Server	9.8	✓	✓	October 26, 2026
CVE-2026-106931	EG Secure Solutions SiteGuard Server Edition OS Command Injection Vulnerability	EG Secure Solutions SiteGuard Server Edition	7.8	✗	✓	October 23, 2026

CVE	NAME	AFFECTED PRODUCT	CVSS 3.x SCORE	ZERO-DAY	PATCH	DUE DATE
CVE-2026-96656	Plex Media Server External Control of File Name or Path Vulnerability	Plex Media Server	7.2	✗	✓	October 23, 2026
CVE-2026-96655	Plex Media Server Server-Side Request Forgery (SSRF) Vulnerability	Plex Media Server	4.3	✗	✓	November 03, 2026
CVE-2026-96654	Plex Media Server Improper Neutralization of Encoded URI Schemes in a Web Page Vulnerability	Plex Media Server	6.5	✗	✓	October 23, 2026
CVE-2026-96652	Plex Media Server Server-Side Request Forgery (SSRF) Vulnerability	Plex Media Server	4.3	✗	✓	November 03, 2026

CVE	NAME	AFFECTED PRODUCT	CVSS 3.x SCORE	ZERO-DAY	PATCH	DUE DATE
CVE-2026-110936	Siemens Software Center Uncontrolled Search Path Element Vulnerability	Siemens Software Center	6.7			November 03, 2026
CVE-2026-102764	BeyondTrust Remote Support Authentication Bypass by Spoofing Vulnerability	BeyondTrust Remote Support	9.8			October 19, 2026
CVE-2025-61624	Fortinet Multiple Products Path Traversal Vulnerability	Fortinet Multiple Products	6.5			October 19, 2026
CVE-2026-21589	Atlassian Multiple Products Files or Directories Accessible to External Parties Vulnerability	Atlassian Multiple Products	7.5			October 18, 2026
CVE-2026-105134	Ahsay AhsayCBS Command Injection Vulnerability	Ahsay AhsayCBS	10			October 17, 2026

CVE	NAME	AFFECTED PRODUCT	CVSS 3.x SCORE	ZERO-DAY	PATCH	DUE DATE
CVE-2026-76519	Cisco Secure Email Gateway Relative Path Traversal Vulnerability	Cisco Secure Email Gateway	9.8	✓	✓	October 17, 2026
CVE-2026-105133	Ahsay AhsayCBS Improper Authentication Vulnerability	Ahsay AhsayCBS	7.3	✓	✓	October 17, 2026
CVE-2026-0322	Palo Alto Networks PAN-OS Code Injection Vulnerability	Palo Alto Networks PAN-OS	7.2	✓	✓	October 17, 2026
CVE-2026-104935	Ivanti Connect Secure Authentication Bypass by Spoofing Vulnerability	Ivanti Connect Secure	8.6	✓	✓	October 16, 2026
CVE-2026-96951	Microsoft Windows Command Injection Vulnerability	Microsoft Windows	8.8	✓	✓	October 16, 2026
CVE-2015-5477	ISC BIND Data Processing Errors Vulnerability	ISC BIND	7.5	✗	✓	October 11, 2026

CVE	NAME	AFFECTED PRODUCT	CVSS 3.x SCORE	ZERO-DAY	PATCH	DUE DATE
CVE-2016-3081	Apache Struts Command Injection Vulnerability	Apache Struts	8.1	✗	✓	October 11, 2026
CVE-2023-22894	Strapi Cleartext Storage of Sensitive Information Vulnerability	Strapi	4.9	✗	✓	October 11, 2026
CVE-2021-3199	ONLYOFFICE Docs Server Path Traversal Vulnerability	ONLYOFFICE Docs	9.8	✗	✓	October 11, 2026
CVE-2015-3306	ProFTPD Improper Access Control Vulnerability	ProFTPD	10	✗	✓	October 11, 2026
CVE-2026-88779	Citrix NetScaler Improper Restriction of Operations within the Bounds of a Memory Buffer Vulnerability	Citrix NetScaler	7.5	✓	✓	October 07, 2026

CVE	NAME	AFFECTED PRODUCT	CVSS 3.x SCORE	ZERO-DAY	PATCH	DUE DATE
CVE-2026-102490	Zammad GmbH Zammad Improper Privilege Management Vulnerability	Zammad GmbH	7.8			October 05, 2026
CVE-2026-102489	Zammad GmbH Zammad Session Fixation Vulnerability	Zammad GmbH Zammad	9.8			October 05, 2026
CVE-2026-104286	Fortinet FortiMail Path Traversal Vulnerability	Fortinet FortiMail	9.8			October 04, 2026

CVEs Details

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2026-118527		Ivanti Connect Secure before versions 25.1.1.3 and 22.8R2.6	UTA0576
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS	cpe:2.3:a:ivanti:connect_secure:*:*:*:*:*:*:*:*	-
Ivanti Connect Secure Generation of Predictable Numbers or Identifiers Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-340	T1190: Exploit Public-Facing Application, T1105: Ingress Tool Transfer, T1068: Exploitation for Privilege Escalation	https://hub.ivanti.com/s/article/Security-Advisory-Ivanti-Connect-Secure-CVE-2026-104935?language=en_US

<table>
<tr><th>CVE ID</th><th>CELEBRITY VULNERABILITY</th><th>AFFECTED PRODUCTS</th><th>ASSOCIATED ACTOR</th></tr>
<tr><td rowspan="3">CVE-2026-111357</td><td></td><td rowspan="2">Ivanti Connect Secure before version 25.1.1.3, and 22.8R2.6</td><td rowspan="2">UTA0576</td></tr>
<tr><td>ZERO-DAY</td></tr>
<tr><td></td><td>AFFECTED CPE</td><td>ASSOCIATED ATTACKS/RANSOMWARE</td></tr>
<tr><td>NAME</td><td>BAS ATTACKS</td><td rowspan="2">cpe:2.3:a:ivanti:connect_secure:*:*:*:*:*:*:*:*</td><td rowspan="2">-</td></tr>
<tr><td rowspan="3">Ivanti Connect Secure Missing Authentication for Critical Function Vulnerability</td><td></td></tr>
<tr><td>CWE ID</td><td>ASSOCIATED TTPs</td><td>PATCH LINK</td></tr>
<tr><td>CWE-306, CWE-862, CWE-345</td><td>T1068: Exploitation for Privilege Escalation, T1071: Application Layer Protocol, T1190: Exploit Public-Facing Application</td><td>https://hub.ivanti.com/s/article/Security-Advisory-Ivanti-Connect-Secure-CVE-2026-104935?language=en_US</td></tr>
</table>

<table>
<tr><th>CVE ID</th><th>CELEBRITY VULNERABILITY</th><th>AFFECTED PRODUCTS</th><th>ASSOCIATED ACTOR</th></tr>
<tr><td rowspan="3">CVE-2026-97229</td><td></td><td rowspan="2">GitLab CE/EE all versions from 19.2 before 19.2.8, 19.3 before 19.3.5, and 19.4 before 19.4.2</td><td rowspan="2">-</td></tr>
<tr><td>ZERO-DAY</td></tr>
<tr><td></td><td>AFFECTED CPE</td><td>ASSOCIATED ATTACKS/RANSOMWARE</td></tr>
<tr><td>NAME</td><td>BAS ATTACKS</td><td rowspan="2">cpe:2.3:a:gitlab:gitlab:*:*:*:*:community:*:*:*, cpe:2.3:a:gitlab:gitlab:*:*:*:*:enterprise:*:*:*</td><td rowspan="2">-</td></tr>
<tr><td rowspan="2">GitLab Community Edition and Enterprise Edition Integer Overflow or Wraparound Vulnerability</td><td></td></tr>
<tr><td>CWE ID</td><td>ASSOCIATED TTPs</td><td>PATCH LINK</td></tr>
<tr><td>CWE-190</td><td>T1190: Exploit Public-Facing Application</td><td>https://docs.gitlab.com/releases/patches/patch-release-gitlab-19-4-2-released/</td></tr>
</table>

<table>
<tr><th>CVE ID</th><th>CELEBRITY VULNERABILITY</th><th>AFFECTED PRODUCTS</th><th>ASSOCIATED ACTOR</th></tr>
<tr><td rowspan="3">CVE-2026-76418</td><td></td><td rowspan="2">Cisco Secure Firewall ASA Software (Before 9.16.4.104, 9.18.4.96, 9.20.4.50, 9.22.3.200, 9.23.1.48, 9.24.1.27 / 9.24.10.1); Cisco Secure Firewall Threat Defense (FTD) Software (Before 7.0.11, 7.2.13, 7.4.9, 7.6.7, 7.7.14, 10.0.3, 10.1.1)</td><td rowspan="2">-</td></tr>
<tr><td>ZERO-DAY</td></tr>
<tr><td></td><td>AFFECTED CPE</td><td>ASSOCIATED ATTACKS/RANSOMWARE</td></tr>
<tr><td>NAME</td><td>BAS ATTACKS</td><td rowspan="2">cpe:2.3:a:cisco:adaptive_security_appliance_software:*:*:*:*:*:*:*:*
cpe:2.3:a:cisco:firepower_threat_defense:*:*:*:*:*:*:*:*</td><td rowspan="2">-</td></tr>
<tr><td rowspan="2">Cisco Secure Firewall ASA Software and Cisco Secure FTD Software Unchecked Return Value to NULL Pointer Dereference Vulnerability</td><td></td></tr>
<tr><td>CWE ID</td><td>ASSOCIATED TTPs</td><td>PATCH LINK</td></tr>
<tr><td>CWE-690</td><td>T1190: Exploit Public-Facing Application, T1499: Endpoint Denial of Service, T1499.004: Application or System Exploitation</td><td>https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-tunnel-dos-s6mgkb75</td></tr>
</table>

<table>
<tr><th>CVE ID</th><th>CELEBRITY VULNERABILITY</th><th>AFFECTED PRODUCTS</th><th>ASSOCIATED ACTOR</th></tr>
<tr><td rowspan="3">CVE-2026-41709</td><td></td><td rowspan="2">VMware Cloud Foundation 9.1.x.x, 9.0.x.x, 5.x before 5.2.4, VMware vSphere Foundation 9.1.x.x, 9.0.x.x, VMware ESX 9.1.x.x before ESXi-9.1.0.0-25370933, 9.0.x.x before ESXi-9.0.2.0100-25595025, 8.0 before ESXi80U3j-25429389, VMware Telco Cloud Platform 5.1.x, 5.0.x</td><td rowspan="2">WARP PANDA</td></tr>
<tr><td>ZERO-DAY</td></tr>
<tr><td></td><td>AFFECTED CPE</td><td>ASSOCIATED ATTACKS/RANSOMWARE</td></tr>
<tr><td>NAME</td><td>BAS ATTACKS</td><td rowspan="2">cpe:2.3:o:vmware:esxi:*:*:*:*:*:*:*:*:*, cpe:2.3:a:vmware:cloud_foundation:*:*:*:*:*:*:*:*:*</td><td rowspan="2">-</td></tr>
<tr><td rowspan="3">Broadcom VMWare ESX Insufficient Logging Vulnerability</td><td></td></tr>
<tr><td>CWE ID</td><td>ASSOCIATED TTPs</td><td>PATCH LINK</td></tr>
<tr><td>CWE-778</td><td>T1211: Exploitation for Defense Evasion, T1562: Impair Defenses, T1562.003: Impair Command History Logging, T1078: Valid Accounts</td><td>https://support.broadcom.com/web/ecx/support-content-notification/-/external/content/SecurityAdvisories/0/38017</td></tr>
</table>

<table>
<tr><th>CVE ID</th><th>CELEBRITY VULNERABILITY</th><th>AFFECTED PRODUCTS</th><th>ASSOCIATED ACTOR</th></tr>
<tr><td rowspan="3">CVE-2026-46300</td><td>Fragnesia</td><td rowspan="2">Linux Kernel (XFRM ESP-in-TCP / 'esp4', 'esp6', 'rxrpc' modules) – impacts AlmaLinux 8/9/10, AlmaLinux Kitten 10, Amazon Linux, CloudLinux, Debian, Fedora, Gentoo, openSUSE, Red Hat Enterprise Linux, SUSE, Ubuntu, and OpenShift</td><td rowspan="2">-</td></tr>
<tr><td>ZERO-DAY</td></tr>
<tr><td></td><td>AFFECTED CPE</td><td>ASSOCIATED ATTACKS/RANSOMWARE</td></tr>
<tr><td>NAME</td><td>BAS ATTACKS</td><td rowspan="2">cpe:2.3:o:linux:linux_kernel:*:*:*:*:*:*:*:*</td><td rowspan="2">-</td></tr>
<tr><td rowspan="3">Linux Kernel Missing Initialization of a Variable Vulnerability</td><td></td></tr>
<tr><td>CWE ID</td><td>ASSOCIATED TTPs</td><td>PATCH LINK</td></tr>
<tr><td>CWE-456</td><td>T1068: Exploitation for Privilege Escalation, T1059: Command and Scripting Interpreter</td><td>https://lore.kernel.org/all/agVpIsaSherjHTYg@sultan-box/</td></tr>
</table>

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2026-48356	PolyShell ZERO-DAY	Adobe Commerce 2.4.9, 2.4.8-p5 and earlier, 2.4.7-p10 and earlier, 2.4.6-p15 and earlier, 2.4.5-p17 and earlier, 2.4.4-p18 and earlier, Adobe Commerce B2B 1.5.3, 1.5.2-p5 and earlier, 1.4.2-p10 and earlier, 1.3.4-p17 and earlier, 1.3.3-p18 and earlier, Magento Open Source, 2.4.9, 2.4.8-p5 and earlier, 2.4.7-p10 and earlier, 2.4.6-p15 and earlier, Adobe Commerce Events, 1.6.0 to 1.20.0	-
	✗	**AFFECTED CPE**	**ASSOCIATED ATTACKS/RANSOMWARE**
NAME	**BAS ATTACKS**	cpe:2.3:a:adobe:commerce:-:*:*:*:*:*:*:*	-
Adobe Commerce and Magento Unrestricted Upload of File with Dangerous Type Vulnerability	✓		
	CWE ID	**ASSOCIATED TTPs**	**PATCH LINK**
	CWE-434	T1190: Exploit Public-Facing Application, T1105: Ingress Tool Transfer, T1036: Masquerading, T1036.008: Masquerade File Type	https://www.adobe.com/trust/security/products/commerce/apsb26-73.html

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2026-111497	Node2Shell/ HTTP2Shell/ Broccoli2Shell	Node.js (22.x before 22.23.4, 24.x before 24.22.1, 26.x before 26.12.1, and End-of-Life versions), Bun (before 1.4.4), Google Brotli (1.0.3 through 1.2.0)	-
	ZERO-DAY		
	✗	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS	cpe:2.3:a:nodejs:node.js:*:*:*:*:*:*:*:*:* cpe:2.3:a:google:brotli:*:*:*:*:*:*:*:*:*	-
Google Brotli Unchecked Return Value Vulnerability	✗		
	CWE ID	ASSOCIATED TTPs	PATCH LINKS
	CWE-252, CWE-787	T1190: Exploit Public-Facing Application, T1059: Command and Scripting Interpreter	https://nodejs.org/en/blog/release/v22.23.4/ , https://nodejs.org/en/blog/release/v24.22.1/ , https://nodejs.org/en/blog/release/v26.12.1/ , https://bun.com/blog/bun-v1.4.4

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2026-109618	PHP2Shell	PHP Group PHP (5.4 through 8.5.11)	Lazarus
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS	cpe:2.3:a:php:php:*:*:*:*:*:*:*:*	-
PHP Memory Corruption Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-416, CWE-755, CWE-824, CWE-1325, CWE-1419	T1190: Exploit Public-Facing Application, T1059: Command and Scripting Interpreter	https://www.php.net/archive/2026.php#2026-10-21-5

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2026-109619	PHP2Shell	PHP Group PHP (5.4 through 8.5.11)	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS	cpe:2.3:a:php:php:*:*:*:*:*:*:*:*	-
PHP Stale Internal Request-State Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-416, CWE-755, CWE-824, CWE-1325, CWE-1419	T1190: Exploit Public-Facing Application, T1059: Command and Scripting Interpreter	https://www.php.net/archive/2026.php#2026-10-21-5

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2026-114625		Arista VeloCloud Orchestrator (VCO) On-Prem (5.2.x before 5.2.3.18, 6.1.x before 6.1.3.10, 6.4.x before 6.4.2.12)	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS	cpe:2.3:a:arista:velocloud_orchestrator:*:*:*:*:*:*:*:*	-
Arista VeloCloud Orchestrator SQL Injection Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-89	T1190: Exploit Public-Facing Application, T1068: Exploitation for Privilege Escalation	https://www.arista.com/en/support/advisories-notices/security-advisory/24838-security-advisory-0199

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2026-110447		Collabora Online Built-in CODE Server before 26.4.303 (richdocumentscode)	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS	cpe:2.3:a:collabora:collabora_online_-_built-in_code_server:*:*:*:*:*:*:nextcloud:*:*	-
Collabora Online – Built-in CODE Server OS Command Injection Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-78	T1190: Exploit Public-Facing Application, T1059: Command and Scripting Interpreter, T1059.004: Unix Shell	https://help.nextcloud.com/t/to-collabora-built-in-user-update-asap/250516

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2026-106931		SiteGuard Server Edition Affected Ver2.20 before Ver8.00 Update 5 (semver) for Apache httpd, Nginx, IIS, Apache httpd on FreeBSD, Nginx on FreeBSD	-
	ZERO-DAY		
		**AFFECTED CPE**	**ASSOCIATED ATTACKS/RANSOMWARE**
NAME	**BAS ATTACKS**	cpe:2.3:a:e-guardian:siteguard:*:*:*:*:server:apache:*:*	-
EG Secure Solutions SiteGuard Server Edition OS Command Injection Vulnerability			
	CWE ID	**ASSOCIATED TTPs**	**PATCH LINK**
	CWE-78	T1068: Exploitation for Privilege Escalation, T1059: Command and Scripting Interpreter, T1059.004: Unix Shell	https://www.eg-secure.co.jp/siteguard/news/alert-202610-1

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2026-96656	Plex2Shell	Plex Media Server (Before 1.43.3.10861)	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS	cpe:2.3:a:plex:media_server:*:*:*:*:*:*:*:*	XMRig myawesomeproxy
Plex Media Server External Control of File Name or Path Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINKS
	CWE-73	T1190: Exploit Public-Facing Application, T1129: Shared Modules, T1574: Hijack Execution Flow	https://forums.plex.tv/t/important-security-update-for-plex-media-server-v1-43-2-and-earlier/942319, https://www.plex.tv/media-server-downloads/

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2026-96655	Plex2Shell	Plex Media Server (Before 1.43.3.10861)	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS	cpe:2.3:a:plex:media_server:*:*:*:*:*:*:*:*	XMRig myawesomeproxy
Plex Media Server Server-Side Request Forgery (SSRF) Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINKS
	CWE-918	T1190: Exploit Public-Facing Application, T1550.001: Application Access Token, T1105: Ingress Tool Transfer	https://forums.plex.tv/t/important-security-update-for-plex-media-server-v1-43-2-and-earlier/942319, https://www.plex.tv/media-server-downloads/

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2026-96654	Plex2Shell	Plex Media Server (Before 1.43.3.10861)	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS	cpe:2.3:a:plex:media_server:*:*:*:*:*:*:*:*	XMRig myawesomeproxy
Plex Media Server Improper Neutralization of Encoded URI Schemes in a Web Page Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINKS
	CWE-84	T1190: Exploit Public-Facing Application	https://forums.plex.tv/t/important-security-update-for-plex-media-server-v1-43-2-and-earlier/942319, https://www.plex.tv/media-server-downloads/

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2026-96652	Plex2Shell	Plex Media Server (Before 1.43.3.10861)	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS	cpe:2.3:a:plex:media_server:*:*:*:*:*:*:*:*	XMRig myawesomeproxy
Plex Media Server Server-Side Request Forgery (SSRF) Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINKS
	CWE-918	T1190: Exploit Public-Facing Application	https://forums.plex.tv/t/important-security-update-for-plex-media-server-v1-43-2-and-earlier/942319, https://www.plex.tv/media-server-downloads/

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2026-110936		Siemens Software Center All versions before V4.0.9.8	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS	cpe:2.3:a:siemens:software_center:*:*:*:*:*:*:*:*	Romulus multi-platform ClickFix campaign
Siemens Software Center Uncontrolled Search Path Element Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINKS
	CWE-427	T1608: Stage Capabilities, T1608.001: Upload Malware, T1204: User Execution, T1204.004: Malicious Copy and Paste, T1059: Command and Scripting Interpreter, T1059001: PowerShell	https://cert-portal.siemens.com/productcert/html/ssa-580366.html, https://productcert.siemens.com/news/2026/10/19/active-exploitation-of-cve-2026-110936-in-siemens-software-center/

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2026-102764		BeyondTrust Remote Support (26.2.3 and prior)	ARMORY CASTLE (aka UNC5221, WARP PANDA)
	ZERO-DAY		
		**AFFECTED CPE**	**ASSOCIATED ATTACKS/RANSOMWARE**
NAME	**BAS ATTACKS**	cpe:2.3:a:beyondtrust:remote_support:*:*:*:*:*:*:*:*	SAWFLY BARECLAW
BeyondTrust Remote Support Authentication Bypass by Spoofing Vulnerability			
	CWE ID	**ASSOCIATED TTPs**	**PATCH LINK**
	CWE-290	T1190: Exploit Public-Facing Application, T1059: Command and Scripting Interpreter	https://www.beyondtrust.com/trust-center/security-advisories/bt26-05

<table>
<tr><th>CVE ID</th><th>CELEBRITY VULNERABILITY</th><th>AFFECTED PRODUCTS</th><th>ASSOCIATED ACTOR</th></tr>
<tr><td rowspan="3">CVE-2025-61624</td><td>✕</td><td rowspan="2">Fortinet FortiOS, FortiPAM, FortiProxy, FortiSwitch Manager</td><td rowspan="2">CL-STA-0954</td></tr>
<tr><td>ZERO-DAY</td></tr>
<tr><td>✕</td><td>AFFECTED CPE</td><td>ASSOCIATED ATTACKS/RANSOMWARE</td></tr>
<tr><td>NAME</td><td>BAS ATTACKS</td><td rowspan="2">cpe:2.3:o:fortinet:fortios:*:*:*:*:*:*:*:*:*,
cpe:2.3:a:fortinet:fortiproxy:*:*:*:*:*:*:*:*:*,
cpe:2.3:o:fortinet:fortipam:*:*:*:*:*:*:*:*:*,
cpe:2.3:a:fortinet:fortiswitchmanager:*:*:*:*:*:*:*:*:*</td><td rowspan="2">PEERSTITCH</td></tr>
<tr><td rowspan="3">Fortinet Multiple Products Path Traversal Vulnerability</td><td>✕</td></tr>
<tr><td>CWE ID</td><td>ASSOCIATED TTPs</td><td>PATCH LINK</td></tr>
<tr><td>CWE-22</td><td>T1190: Exploit Public-Facing Application, T1068: Exploitation for Privilege Escalation</td><td>https://fortiguard.fortinet.com/psirt/FG-IR-26-122</td></tr>
</table>

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2026-21589	✗	Atlassian Bitbucket Data Center Version before 9.4.26,10.2.8, 10.5.1, Confluence Data Center Version before 9.2.26, 10.2.19, Jira Service Management Data Center Version before 5.12.40,10.3.26, 11.3.12, Jira Software Data Center Version before 9.12.40, 10.3.26,11.3.12, Bamboo Data Center Versions before 10.2.24,12.1.12, Crowd Data Center Version before 6.3.7, 7.0.3,7.1.7,7.2.4, Crucible Version before 4.9.15 and Fisheye Version before 4.9.15	-
	ZERO-DAY		
	✗	**AFFECTED CPE**	**ASSOCIATED ATTACKS/RANSOMWARE**
NAME	**BAS ATTACKS**	cpe:2.3:a:atlassian:bitbucket:*:*:*:*:*:data_center:*:*:*, cpe:2.3:a:atlassian:confluence:*:*:*:*:*:data_center:*:*:*, cpe:2.3:a:atlassian:jira_service_management:*:*:*:*:*:data_center:*:*:*, cpe:2.3:a:atlassian:jira_software:*:*:*:*:*:data_center:*:*:*, cpe:2.3:a:atlassian:bamboo:*:*:*:*:*:data_center:*:*:*, cpe:2.3:a:atlassian:crowd:*:*:*:*:*:data_center:*:*:*, cpe:2.3:a:atlassian:crucible:*:*:*:*:*:*:*:*:*, cpe:2.3:a:atlassian:fisheye:*:*:*:*:*:*:*:*:*	-
Atlassian Multiple Products Files or Directories Accessible to External Parties Vulnerability	✓		
	CWE ID	**ASSOCIATED TTPs**	**PATCH LINK**
	CWE-552	T1190: Exploit Public-Facing Application, T1552: Unsecured Credentials	https://confluence.atlassian.com/security/cve-2026-21589-arbitrary-file-access-vulnerability-impacts-multiple-products-1870495748.html

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2026-105134		Ahsay AhsayCBS (v10 builds before hotfix 10.3.4.45)	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS	cpe:2.3:a:ahsay:ahsaycbs:*:*:*:*:*:*:*:*	XMRig
Ahsay AhsayCBS Command Injection Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-77, CWE-78	T1190: Exploit Public-Facing Application, T1059: Command and Scripting Interpreter	https://idp3.ahsay.com/idp/Authn/RemoteUser

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2026-76519	✗	Cisco Secure Email Gateway (AsyncOS 15.5 before 15.5.5-014, 16.0 all releases, 16.5 before 16.5.0-780; Content Scanner Tools before 25.3.0.5525)	-
	ZERO-DAY		
	✓	**AFFECTED CPE**	**ASSOCIATED ATTACKS/RANSOMWARE**
NAME	**BAS ATTACKS**	cpe:2.3:a:cisco:secure_email_gateway:*:*:*:*:*:*:*:*	-
Cisco Secure Email Gateway Relative Path Traversal Vulnerability	✗		
	CWE ID	**ASSOCIATED TTPs**	**PATCH LINK**
	CWE-23	T1190: Exploit Public-Facing Application, T1059: Command and Scripting Interpreter, T1068: Exploitation for Privilege Escalation	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-esa-afw-zqYJkjxp

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2026-105133		Ahsay AhsayCBS (v10 builds before hotfix 10.3.4.45)	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS	cpe:2.3:a:ahsay:ahsaycbs:*:*:*:*:*:*:*:*	XMRig
Ahsay AhsayCBS Improper Authentication Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-287	T1190: Exploit Public-Facing Application, T1059: Command and Scripting Interpreter	https://idp3.ahsay.com/idp/Authn/RemoteUser

<table>
<tr><th>CVE ID</th><th>CELEBRITY VULNERABILITY</th><th>AFFECTED PRODUCTS</th><th>ASSOCIATED ACTOR</th></tr>
<tr><td rowspan="3">CVE-2026-0322</td><td></td><td rowspan="2">Palo Alto Networks PAN-OS 12.2 (Before 12.2.4), 12.1 (Before 12.1.4-h12, 12.1.7-h8, 12.1.10-h2), 11.2 (Before 11.2.4-h22, 11.2.7-h21, 11.2.10-h15, 11.2.13-h3, 11.2.16), 11.1 (Before 11.1.4-h37, 11.1.6-h39, 11.1.7-h11, 11.1.10-h35, 11.1.13-h15, 11.1.16-h3), 10.2 (Before 10.2.7-h38, 10.2.10-h41, 10.2.13-h26, 10.2.16-h11, 10.2.18-h12) on PA-Series, VM-Series and Panorama</td><td rowspan="2">-</td></tr>
<tr><td>ZERO-DAY</td></tr>
<tr><td></td><td>AFFECTED CPE</td><td>ASSOCIATED ATTACKS/RANSOMWARE</td></tr>
<tr><td>NAME</td><td>BAS ATTACKS</td><td rowspan="2">cpe:2.3:o:palo_alto_networks:pan-os:*:*:*:*:*:*:*:*</td><td rowspan="2">-</td></tr>
<tr><td rowspan="3">Palo Alto Networks PAN-OS Code Injection Vulnerability</td><td></td></tr>
<tr><td>CWE ID</td><td>ASSOCIATED TTPs</td><td>PATCH LINK</td></tr>
<tr><td>CWE-94</td><td>T1190: Exploit Public-Facing Application, T1059: Command and Scripting Interpreter, T1068: Exploitation for Privilege Escalation</td><td>https://security.paloaltonetworks.com/CVE-2026-0322</td></tr>
</table>

<table>
<tr><th>CVE ID</th><th>CELEBRITY VULNERABILITY</th><th>AFFECTED PRODUCTS</th><th>ASSOCIATED ACTOR</th></tr>
<tr><td rowspan="3">CVE-2026-104935</td><td></td><td rowspan="2">Ivanti Connect Secure (22.8R2.4 and prior; 25.1.1.1 on ISA6000/ISA8000; 25.1.2.2 and prior)</td><td rowspan="2">UTA0576</td></tr>
<tr><td>ZERO-DAY</td></tr>
<tr><td></td><td>AFFECTED CPE</td><td>ASSOCIATED ATTACKS/RANSOMWARE</td></tr>
<tr><td>NAME</td><td>BAS ATTACKS</td><td rowspan="2">cpe:2.3:a:ivanti:connect_secure:*:*:*:*:*:*:*:*:*</td><td rowspan="2">-</td></tr>
<tr><td rowspan="3">Ivanti Connect Secure Authentication Bypass by Spoofing Vulnerability</td><td></td></tr>
<tr><td>CWE ID</td><td>ASSOCIATED TTPs</td><td>PATCH LINK</td></tr>
<tr><td>CWE-290</td><td>T1190: Exploit Public-Facing Application, T1059: Command and Scripting Interpreter, T1068: Exploitation for Privilege Escalation</td><td>https://hub.ivanti.com/s/article/Security-Advisory-Ivanti-Connect-Secure-CVE-2026-104935?language=en_US</td></tr>
</table>

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2026-96951		Windows 10 - 11 26H2, Windows Server 2012, 2016, 2019, 2025, 2022, Outlook.com	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS	cpe:2.3:a:microsoft:outlook_web:-:*:*:*:*:*:*:*, cpe:2.3:o:microsoft:windows:*:*:*:*:*:*:*:*, cpe:2.3:o:microsoft:windows_server:*:*:*:*:*:*:*:*	-
Microsoft Windows Command Injection Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-77	T1059: Command and Scripting Interpreter, T1068: Exploitation for Privilege Escalation	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-96951

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2015-5477		ISC BIND 9.x before 9.9.7-P2 and 9.10.x before 9.10.2-P3	Flax Typhoon
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS	cpe:2.3:o:juniper:junos:*:*:*:*:*:*:*:*	-
ISC BIND Data Processing Errors Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-19	T1499: Endpoint Denial of Service, T1499.004: Application or System Exploitation, T1588: Obtain Capabilities, T1588.005: Exploits	https://kb.isc.org/article/AA-01272

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2016-3081		Apache Struts 2.3.19 to 2.3.20.2, 2.3.21 to 2.3.24.1, and 2.3.25 to 2.3.28	Flax Typhoon
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS	cpe:2.3:o:huawei:agile_controller-campus_firmware:-:*:*:*:*:*:*:*:*, cpe:2.3:h:huawei:agile_controller-campus:-:*:*:*:*:*:*:*:*	-
Apache Struts Command Injection Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-77	T1588: Obtain Capabilities, T1588.005: Exploits, T1190: Exploit Public-Facing Application	https://cwiki.apache.org/confluence/spaces/WW/pages/62693266/S2-032

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2023-22894		Strapi through 4.5.5	Flax Typhoon
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS	cpe:2.3:a:strapi:strapi:*:*:*:*:*:*:*:*	-
Strapi Cleartext Storage of Sensitive Information Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-312	T1588: Obtain Capabilities, T1588.005: Exploits, T1190: Exploit Public-Facing Application, T1212: Exploitation for Credential Access	https://github.com/strapi/strapi/releases

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2021-3199		ONLYOFFICE Document Server before 5.6.3	Flax Typhoon
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS	cpe:2.3:a:onlyoffice:document_server:*:*:*:*:*:*:*:*	-
ONLYOFFICE Docs Server Path Traversal Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-22	T1588: Obtain Capabilities, T1588.005: Exploits, T1190: Exploit Public-Facing Application	https://github.com/ONLYOFFICE/DocumentServer/blob/903fe5ab7a275bd69c3c3346af2d21cf87ebeabf/CHANGELOG.md#563

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2015-3306		ProFTPD 1.3.5	Flax Typhoon
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS	cpe:2.3:a:proftpd:proftpd:1.3.5:*:*:*:*:*:*:*	-
ProFTPD Improper Access Control Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-284	T1588: Obtain Capabilities, T1588.005: Exploits, T1190: Exploit Public-Facing Application	https://github.com/proftpd/proftpd/releases

<table>
<tr><th>CVE ID</th><th>CELEBRITY VULNERABILITY</th><th>AFFECTED PRODUCTS</th><th>ASSOCIATED ACTOR</th></tr>
<tr><td rowspan="3">CVE-2026-88779</td><td></td><td rowspan="2">Citrix NetScaler ADC and NetScaler Gateway 14.1 (Before 14.1-73.41), Citrix NetScaler ADC and NetScaler Gateway 13.1 (Before 13.1-64.28), Citrix NetScaler ADC 14.1-FIPS (Before 14.1-73.41 FIPS), Citrix NetScaler ADC 13.1-FIPS and 13.1-NDcPP (Before 13.1-37.282)</td><td rowspan="2">-</td></tr>
<tr><td>ZERO-DAY</td></tr>
<tr><td></td><td>AFFECTED CPE</td><td>ASSOCIATED ATTACKS/RANSOMWARE</td></tr>
<tr><td>NAME</td><td>BAS ATTACKS</td><td rowspan="2">cpe:2.3:a:citrix:netscaler_application_delivery_controller:*:*:*:*:*:*:*:*:*,
cpe:2.3:a:citrix:netscaler_gateway:*:*:*:*:*:*:*:*:*,
cpe:2.3:a:citrix:netscaler_application_delivery_controller:*:*:*:*:fips:*:*:*,
cpe:2.3:a:citrix:netscaler_application_delivery_controller:*:*:*:*:ndcpp:*:*:*</td><td rowspan="2">-</td></tr>
<tr><td rowspan="2">Citrix NetScaler Improper Restriction of Operations within the Bounds of a Memory Buffer Vulnerability</td><td></td></tr>
<tr><td>CWE ID</td><td>ASSOCIATED TTPs</td><td>PATCH LINK</td></tr>
<tr><td>CWE-119</td><td>T1190: Exploit Public-Facing Application, T1059: Command and Scripting Interpreter, T1059.004: Unix Shell, T1105: Ingress Tool Transfer, T1505: Server Software Component</td><td>https://support.citrix.com/external/article/CTX697174/citrix-netscaler-adc-and-citrix-netscale.html</td></tr>
</table>

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2026-102490		Zammad GmbH Zammad Affected 1.5.0 before 7.2.2 (semver)	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS	cpe:2.3:a:zammad:zammad:*:*:*:*:*:*:*:*	-
Zammad GmbH Zammad Improper Privilege Management Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-269	T1190: Exploit Public-Facing Application, T1059: Command and Scripting Interpreter, T1059.004: Unix Shell	https://zammad.com/en/advisories/cve-2026-102489-cve-2026-102490

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2026-102489		Zammad versions 6.3.0 to 6.5.4	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS	cpe:2.3:a:zammad:zammad:*:*:*:*:*:*:*:*	-
Zammad GmbH Zammad Session Fixation Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINKS
	CWE-384	T1190 : Exploit Public-Facing Application, T1539: Steal Web Session Cookie	https://community.zammad.org/t/take-care-local-privilege-escalation-cve-2026-102490-is-reported-as-being-actively-exploited/21297/2, https://zammad.com/en/advisories/cve-2026-102489-cve-2026-102490

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2026-104286		Fortinet FortiMail 8.0.0 through 8.0.1, 7.6.0 through 7.6.6, 7.4.0 through 7.4.8, 7.2.0 through 7.2.9	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS	cpe:2.3:a:fortinet:fortimail:*:*:*:*:*:*:*:*	-
Fortinet FortiMail Path Traversal Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-22, CWE-158	T1190: Exploit Public-Facing Application, T1059: Command and Scripting Interpreter	https://fortiguard.fortinet.com/psirt/FG-IR-26-175

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

November 05, 2026 • 10:00 AM

© 2026 All Rights are Reserved by Hive Pro

More at www.hivepro.com