



HiveForce Labs

CISA

KNOWN

EXPLOITED

VULNERABILITY

CATALOG

August 2026

Table of Contents

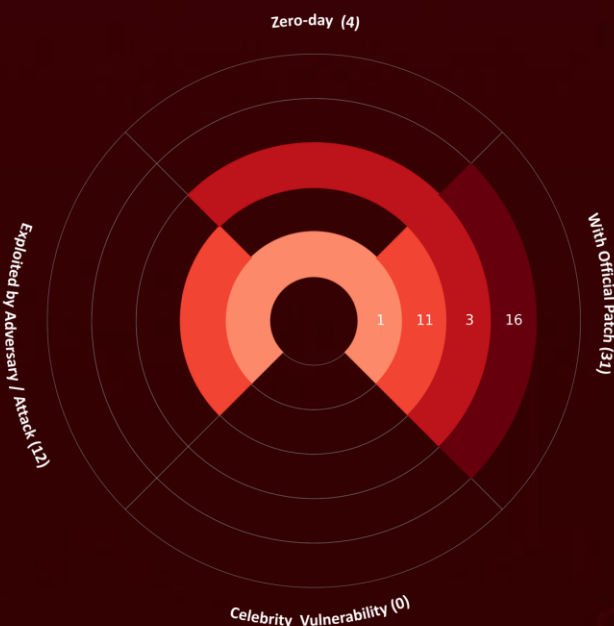
<u>Summary</u>	03
<u>CVEs List</u>	04
<u>CVEs Details</u>	10
<u>Recommendations</u>	35
<u>References</u>	36
<u>Appendix</u>	36
<u>What Next?</u>	37

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 **August 2026**, **31** vulnerabilities met the criteria for inclusion in CISA's KEV catalog. Of these, **4** are **zero-day** vulnerabilities; **12** have been **exploited** by a threat actor and employed in attacks.

31
Known Exploited
Vulnerabilities





CVEs List

CVE	NAME	AFFECTED PRODUCT	CVSS 3.x SCORE	ZERO-DAY	PATCH	DUE DATE
<u>CVE-2026-82078</u>	PaperCut NG/MF Unsafe Reflection Vulnerability	PaperCut NG/MF	9.1			September 14, 2026
<u>CVE-2026-81578</u>	PaperCut NG/MF Missing Authentication for Critical Function Vulnerability	PaperCut NG/MF	9.8			September 14, 2026
<u>CVE-2023-49105</u>	ownCloud Improper Authentication Vulnerability	ownCloud	9.8			August 30, 2026
CVE-2026-53362	Linux Kernel Unspecified Vulnerability	Linux Kernel	7.8			August 30, 2026
CVE-2026-66384	JFrog Artifactory Improper Limitation of a Pathname to a Restricted Directory Vulnerability	JFrog Artifactory	5.3			September 10, 2026

CVE	NAME	AFFECTED PRODUCT	CVSS 3.x SCORE	ZERO-DAY	PATCH	DUE DATE
CVE-2021-23758	Ajax.NET Professional Deserialization of Untrusted Data Vulnerability	Ajax.NET Professional	9.8			September 09, 2026
CVE-2015-3246	Red Hat Libuser Race Condition Vulnerability	Red Hat Libuser	5.1			September 09, 2026
CVE-2015-5287	Red Hat Automatic Bug Reporting Tool Privilege Escalation Vulnerability	Red Hat Automatic Bug Reporting Tool	7.8			September 09, 2026
CVE-2022-0995	Linux Kernel Out-of-Bounds Write Vulnerability	Linux Kernel	7.8			September 09, 2026
CVE-2026-8452	Citrix NetScaler ADC and NetScaler Gateway Improper Restriction of Operations within the Bounds of a Memory Buffer Vulnerability	Citrix NetScaler ADC and NetScaler Gateway	9.8			August 29, 2026

CVE	NAME	AFFECTED PRODUCT	CVSS 3.x SCORE	ZERO-DAY	PATCH	DUE DATE
CVE-2019-1068	Microsoft SQL Server Remote Code Execution Vulnerability	Microsoft SQL Server	8.8			August 29, 2026
<u>CVE-2026-60004</u>	Gitea Code Injection Vulnerability	Gitea	9.8			August 28, 2026
<u>CVE-2026-21962</u>	Oracle HTTP Server and Oracle Weblogic Server Proxy Plug-in Improper Access Control Vulnerability	Oracle HTTP Server and Oracle Weblogic Server Proxy Plug-in	10			August 27, 2026
CVE-2026-73570	Zimbra Collaboration Suite (ZCS) OS Command Injection Vulnerability	Synacor Zimbra Collaboration Suite (ZCS)	8.9			August 24, 2026
<u>CVE-2026-72530</u>	TrueConf Server Code Injection Vulnerability	TrueConf Server	9			September 03, 2026

CVE	NAME	AFFECTED PRODUCT	CVSS 3.x SCORE	ZERO-DAY	PATCH	DUE DATE
CVE-2026-72529	TrueConf Server Missing Authentication for Critical Function Vulnerability	TrueConf Server	9.8			August 23, 2026
CVE-2026-64849	MLflow Server-Side Request Forgery Vulnerability	MLflow	9.3			September 02, 2026
CVE-2026-33824	Microsoft Internet Key Exchange (IKE) Service Extensions Double Free Vulnerability	Microsoft Internet Key Exchange (IKE) Service Extensions	9.8			August 21, 2026
CVE-2026-59310	Broadcom VMware vCenter Path Traversal Vulnerability	Broadcom VMware vCenter	9.8			August 21, 2026
CVE-2026-55040	Microsoft SharePoint Weak Authentication Vulnerability	Microsoft SharePoint	9.1			August 21, 2026
CVE-2026-65400	Apple macOS Improper Authentication Vulnerability	Apple macOS	9.8			August 21, 2026

CVE	NAME	AFFECTED PRODUCT	CVSS 3.x SCORE	ZERO-DAY	PATCH	DUE DATE
CVE-2025-62593	Ray-Project Ray Code Injection Vulnerability	Ray-Project Ray	8.8			August 20, 2026
CVE-2026-20349	Cisco Secure Firewall Adaptive Security Appliance (ASA) and Secure Firewall Threat Defense (FTD) Heap Inspection Vulnerability	Cisco Secure Firewall Adaptive Security Appliance (ASA) and Secure Firewall Threat Defense (FTD)	8.6			August 14, 2026
<u>CVE-2026-68820</u>	Microsoft Windows Ancillary Function Driver for WinSock Use-After-Free Vulnerability	Microsoft Windows Ancillary Function Driver for WinSock	7			August 25, 2026
CVE-2026-72898	Metabase SQL Injection Vulnerability	Metabase	10			August 14, 2026
CVE-2026-8037	Progress LoadMaster Command Injection Vulnerability	Progress LoadMaster	9.8			August 10, 2026

CVE	NAME	AFFECTED PRODUCT	CVSS 3.x SCORE	ZERO-DAY	PATCH	DUE DATE
<u>CVE-2026-63077</u>	JetBrains TeamCity Deserialization of Untrusted Data Vulnerability	JetBrainsTeamCity	9.8			August 08, 2026
<u>CVE-2026-18556</u>	N-able N-central Authentication Bypass Using an Alternate Path or Channel Vulnerability	N-able N-central	7.4			August 07, 2026
CVE-2026-34486	Apache Tomcat Missing Encryption of Sensitive Data Vulnerability	Apache Tomcat	7.5			August 07, 2026
CVE-2026-9198	IBM Langflow Code Injection Vulnerability	IBM Langflow	9.8			August 07, 2026
<u>CVE-2026-18577</u>	N-able N-central Authentication Bypass Using an Alternate Path or Channel Vulnerability	N-able N-central	8.1			August 06, 2026



CVEs Details

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
<u>CVE-2026-82078</u>		All versions of PaperCut NG and PaperCut MF	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS	cpe:2.3:a:papercut:papercut_ng:*:*:*:*:*:* cpe:2.3:a:papercut:papercut_mf:*:*:*:*:*:*	-
PaperCut NG/MF Unsafe Reflection Vulnerability			
	CWE ID		
	CWE-470	T1190:Exploit Public-Facing Application, T1059:Command and Scripting Interpreter, T1070:Indicator Removal	https://www.papercut.com/kb/Main/security-bulletin-27-aug-2026-urgent-security-advisory/

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
<u>CVE-2026-81578</u>		All versions of PaperCut NG and PaperCut MF	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS		
PaperCut NG/MF Missing Authentication for Critical Function Vulnerability		cpe:2.3:a:papercut:papercut_ng:*:*:*:*:*:* cpe:2.3:a:papercut:papercut_mf:*:*:*:*:*:*	-
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-306	T1190:Exploit Public-Facing Application, T1562:Impair Defenses	https://www.papercut.com/kb/Main/security-bulletin-27-aug-2026-urgent-security-advisory/

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
<u>CVE-2023-49105</u>		ownCloud Server: 10.6.0 - 10.13.0	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS	cpe:2.3:a:owncloud:core:*:*:*:*:*:*	-
ownCloud Improper Authentication Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-287	T1589: Gather Victim Identity Information	https://owncloud.com/download-server

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2026-53362		Linux kernel	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS	cpe:2.3:o:linux:linux_kernel:*:*:*:*:*:*	-
Linux Kernel Unspecified Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-122, CWE-787	T1068: Exploitation for Privilege Escalation	https://git.kernel.org/pub/scm/linux/kernel/git/stable/linux.git/commit/?id=e9eacf19281ea2498b36291b56c9606118c2d74e

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2026-66384		JFrog Artifactory versions before 7.146.35 and the 7.161.0 through 7.161.16 line	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS	cpe:2.3:a:jfrog:artifactory:*:*:*:*:*:*:*:*	-
JFrog Artifactory Improper Limitation of a Pathname to a Restricted Directory Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-22	T1552: Unsecured Credentials	https://jfrog.com/community/download-artifactory-oss/

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2021-23758		All versions of the ajaxpro.2 package before 21.11.29.1	UAT-10147
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS	cpe:2.3:a:ajaxpro.2_project:ajaxpro.2:*:*:*:*:*:.net:*.* cpe:2.3:a:michaelschwarz:ajax.net_professional:*:*:*:*:*:.net:*.*	NoodleRAT SPECTRE Meterpreter
Ajax.NET Professional Deserialization of Untrusted Data Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-502	T1190: Exploit Public-Facing Application, T1059: Command and Scripting Interpreter	https://github.com/michaelschwarz/Ajax.NET-Professional/releases/

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2015-3246		libuser before 0.56.13-8 and 0.60 before 0.60-7	UAT-10147
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS	cpe:2.3:o:redhat:enterprise_linux:*:*:*:*:* cpe:2.3:o:opensuse:opensuse:13.2:*:*:*:*:* cpe:2.3:a:libuser_project:libuser:*:*:*:*:*	NoodleRAT SPECTRE Meterpreter
Red Hat Libuser Race Condition Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-264, CWE-367	T1068: Exploitation for Privilege Escalation	https://pkgs.org/download/libuser

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2015-5287		Automatic Bug Reporting Tool (ABRT) before 2.7.1	UAT-10147
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS	cpe:2.3:a:redhat:automatic_bug_reporting_tool:*:*:*:*:* cpe:2.3:o:redhat:enterprise_linux:*:*:*:*:*	NoodleRAT SPECTRE Meterpreter
Red Hat Automatic Bug Reporting Tool Privilege Escalation Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-59	T1068: Exploitation for Privilege Escalation	https://github.com/abrt/abrt/releases

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2022-0995		Linux Kernel versions through 5.17:rc7	UAT-10147
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS	cpe:2.3:o:linux:linux_kernel:*:*:*.*.*.*.*.*	NoodleRAT SPECTRE Meterpreter
Linux Kernel Out-of-Bounds Write Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-787	T1499: Endpoint Denial of Service T1068: Exploitation for Privilege Escalation	https://git.kernel.org/pub/scm/linux/kernel/git/torvalds/linux.git/commit/?id=93ce93587d36493f2f86921fa79921b3cba63fbb

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2026-8452		NetScaler ADC and NetScaler Gateway 14.1 BEFORE 14.1-72.61	-
	ZERO-DAY	NetScaler ADC and NetScaler Gateway 13.1 BEFORE 13.1-63.18 NetScaler ADC FIPS BEFORE 14.1-72.61 FIPS NetScaler ADC FIPS and NDcPP BEFORE 13.1-37.272	
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS	cpe:2.3:a:citrix:netScaler_application_delivery_controller:*:*:*:*:fips:*:*:* cpe:2.3:a:citrix:netScaler_application_delivery_controller:*:*:*:*:ndcPP:*:*:* cpe:2.3:a:citrix:netScaler_application_delivery_controller:*:*:*:*:*:*:* cpe:2.3:a:citrix:netScaler_gateway:*:*:*:*:*:*:*	-
Citrix NetScaler ADC and NetScaler Gateway Improper Restriction of Operations within the Bounds of a Memory Buffer Vulnerability		ASSOCIATED TTPs	PATCH LINK
	CWE-119	T1190: Exploit Public-Facing Application, T1203: Exploitation for Client Execution	https://support.citrix.com/support-home/kbsearch/article?articleNumber=CTX696604

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2019-1068		Microsoft SQL Server 2014 Service Pack 3 for 32-bit Systems (GDR), Microsoft SQL Server 2014 Service Pack 3 for 32-bit Systems (CU 4), Microsoft SQL Server 2014 Service Pack 3 for x64-based Systems (GDR), Microsoft SQL Server 2014 Service Pack 3 for x64-based Systems (CU), Microsoft SQL Server 2014 Service Pack 2 for x64-based Systems (GDR), Microsoft SQL Server 2014 Service Pack 2 for x64-based Systems (CU), Microsoft SQL Server 2014 Service Pack 2 for 32-bit Systems (CU), Microsoft SQL Server 2014 Service Pack 2 for 32-bit Systems (GDR), Microsoft SQL Server 2016 for x64-based Systems Service Pack 2 (GDR), Microsoft SQL Server 2016 for x64-based Systems Service Pack 2 (CU), Microsoft SQL Server 2017 for x64-based Systems (CU), Microsoft SQL Server 2017 for x64-based Systems (GDR), Microsoft SQL Server 2016 for x64-based Systems Service Pack 1 (CU), Microsoft SQL Server 2016 for x64-based Systems Service Pack 1 (GDR)	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS	cpe:2.3:a:microsoft:sql_server:*.*.*.*.*.*.*.*	-
Microsoft SQL Server Remote Code Execution Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-20	T1190: Exploit Public-Facing Application, T1059: Command and Scripting Interpreter	https://msrc.microsoft.com/update-guide/en-US/advisory/CVE-2019-1068

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
<u>CVE-2026-21962</u>		Oracle HTTP Server, Oracle WebLogic Server Proxy Plug-in for Apache HTTP Server (12.2.1.4.0, 14.1.1.0.0, 14.1.2.0.0); WebLogic Server Proxy Plug-in for Microsoft IIS (12.2.1.4.0)	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS		
Oracle HTTP Server and Oracle Weblogic Server Proxy Plug-in Improper Access Control Vulnerability		cpe:2.3:a:oracle:http_server:*:*:*:*:*:* cpe:2.3:a:oracle:weblogic_server_proxy Plug-in:*:*:*:*:*:*	-
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-284	T1190:Exploit Public-Facing Application, T1059:Command and Scripting Interpreter	https://www.oracle.com/security-alerts/cpujan2026.html

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2026-73570		Zimbra Collaboration (ZCS) before 10.1.20	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS	cpe:2.3:a:synacor:zimbra_collaboration_suite:*:*:*:*:*:*	-
Zimbra Collaboration Suite (ZCS) OS Command Injection Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-78	T1190:Exploit Public-Facing Application, T1059:Command and Scripting Interpreter	https://wiki.zimbra.com/wiki/Zimbra_Releases/10.1.20

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2026-72530		TrueConf server versions 5.3.X to 5.3.9, 5.4.X to 5.4.9, 5.5.X to 5.5.5, and earlier	Head Mare
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS	cpe:2.3:a:trueconf:trueconf_server:*:*:*:*:windows:*:* cpe:2.3:a:trueconf:trueconf_server:*:*:*:*:linux_kernel:*:*	PhantomCore PhantomGraph
TrueConf Server Code Injection Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-94	T1190:Exploit Public-Facing Application, T1059:Command and Scripting Interpreter	https://trueconf.com/products/tcsf/trueconf-server-free.html

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2026-72529		TrueConf server versions 5.3.X to 5.3.9, 5.4.X to 5.4.9, 5.5.X to 5.5.5, and earlier	Head Mare
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS	cpe:2.3:a:trueconf:trueconf_server:*:*:*:*:windows:*:* cpe:2.3:a:trueconf:trueconf_server:*:*:*:*:linux_kernel:*:*	PhantomCore PhantomGraph
TrueConf Server Missing Authentication for Critical Function Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-306	T1190:Exploit Public-Facing Application, T1059:Command and Scripting Interpreter	https://trueconf.com/products/tcsf/trueconf-server-free.html

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2026-64849		MLflow (Before 3.15.0)	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS	cpe:2.3:a:mlflow:mlflow:*:*:*:*:*:*:*	-
MLflow Server-Side Request Forgery Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINKS
	CWE-918	T1190: Exploit Public-Facing Application, T1552: Unsecured Credentials	https://github.com/mlflow/mlflow/releases/tag/v3.15.0

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2026-33824		Windows Server 2016, 2019, 2022, 2025; Windows 10 -11 25H2	knaithe (aka KnYuan)
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS	cpe:2.3:o:microsoft:windows:*:*:*:*:*:*	-
Microsoft Internet Key Exchange (IKE) Service Extensions Double Free Vulnerability		cpe:2.3:o:microsoft:*:*:*:*:*:*:*:*	
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-415	T1190: Exploit Public-Facing Application	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-33824

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
<u>CVE-2026-59310</u>		VMware vCenter (9.1.x.x, 9.0.x.x, 8.0, 7.0), VMware Cloud Foundation (9.1.x.x, 9.0.x.x, 5.x), VMware vSphere Foundation (9.1.x.x, 9.0.x.x), VMware Telco Cloud Platform (3.0, 4.x, 5.0.x, 5.1.x), VMware Telco Cloud Infrastructure (3.0)	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS	cpe:2.3:a:vmware:vcenter_server:*:*:*:*:*:* cpe:2.3:a:vmware:cloud_foundation:*:*:*:*:*:* cpe:2.3:a:vmware:vsphere_foundation:*:*:*:*:*:* cpe:2.3:a:vmware:telco_cloud_platform:*:*:*:*:*:* cpe:2.3:a:vmware:telco_cloud_infrastructure:*:*:*:*:*:*	Babuk-derived ESXi ransomware
Broadcom VMware vCenter Path Traversal Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-22	T1190: Exploit Public-Facing Application, T1053: Scheduled Task/Job, T1059: Command and Scripting Interpreter	https://support.broadcom.com/web/ecx/support-content-notification/-/external/content/SecurityAdvisories/0/3801Z

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
<u>CVE-2026-65400</u>		Apple macOS Sonoma (Before 14.8.9), macOS Sequoia (Before 15.7.9), macOS Tahoe (Before 26.6.1)	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS	cpe:2.3:o:apple:macos:*:*:*:*:*:*	Monero Miner
Apple macOS Improper Authentication Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINKS
	CWE-287	T1190: Exploit Public-Facing Application, T1133: External Remote Services, T1496: Resource Hijacking	https://support.apple.com/en-us/148170 , https://support.apple.com/en-us/148171 , https://support.apple.com/en-us/148172

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2025-62593		Ray Prior to version 2.52.0	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS	cpe:2.3:a:anyscale:ray:*:*:*:*:*:*:*	RondoDox ShadowRay 2.0
Ray-Project Ray Code Injection Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-94, CWE-352	T1189: Drive-by Compromise, T1059: Command and Scripting Interpreter	https://github.com/ray-project/ray/releases

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2026-20349		Cisco Secure Firewall Adaptive Security Appliance (ASA) Software, Cisco Secure Firewall Threat Defense (FTD) Software	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS	cpe:2.3:o:cisco:adaptive_security_appliance_software:*:*:*:*:*:*:*	-
Cisco Secure Firewall Adaptive Security Appliance (ASA) and Secure Firewall Threat Defense (FTD) Heap Inspection Vulnerability		cpe:2.3:a:cisco:secure_firewall_threat_defense:*:*:*:*:*:*	-
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-244	T1190: Exploit Public-Facing Application, T1499: Endpoint Denial of Service	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-vpn-dos-dzv4mQFF

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
<u>CVE-2026-68820</u>		Windows Server 2012, 2016, 2019, 2022, 2025, Windows 10- 11 26H1	Lazarus
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS	cpe:2.3:o:microsoft:windows:*:*:*:*:* cpe:2.3:o:microsoft:windows_server:*:*:*:*:*:*	Troy FudModule RelayShell MISTPEN ForestTiger
Microsoft Windows Ancillary Function Driver for WinSock Use-After-Free Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-416	T1190: Exploit Public-Facing Application, T1068: Exploitation for Privilege Escalation	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-68820

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2026-72898		Metabase both open-source and Enterprise editions versions prior to x.58.24, x.59.21, x.60.17, x.61.11, x.62.9, x.63.5	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS	cpe:2.3:a:metabase:metabase:*:*:*:*:*:*:*:*	-
Metabase SQL Injection Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-89	T1190: Exploit Public-Facing Application, T1068: Exploitation for Privilege Escalation	https://github.com/metabase/metabase/security/advisories/GHSA-vwf4-m7j8-wcjf

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2026-8037		Kemp LoadMaster: GA v7.2.63.1 and older Kemp LoadMaster: LTSF v7.2.54.17 and older	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS		
Progress LoadMaster Command Injection Vulnerability		cpe:2.3:a:progress:connection_manager_for_objectscale:*:*:*:*:* cpe:2.3:a:progress:ecs_connection_manager:*:*:*:*:* cpe:2.3:a:progress:moveit_web_application_firewall:*:*:*:*:* cpe:2.3:o:progress:loadmaster:*:*:*:*:*	-
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-77	T1190: Exploit Public-Facing Application, T1059: Command and Scripting Interpreter	https://community.progress.com/s/article/LoadMaster-Critical-Security-Bulletin-June-2026-CVE-2026-8037-CVE-2026-33691

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
<u>CVE-2026-63077</u>		JetBrains TeamCity On-Premises (all versions before 2025.11.7 and before 2026.1.3)	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS	cpe:2.3:a:jetbrains:teamcity:*:*.*.*.*.*.*.*	-
JetBrains TeamCity Deserialization of Untrusted Data Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-502	T1190: Exploit Public-Facing Application, T1195: Supply Chain Compromise, T1059: Command and Scripting Interpreter	https://www.jetbrains.com/teamcity/download/other/

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
<u>CVE-2026-18556</u>		N-able N-central (Before 2026.2)	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS	cpe:2.3:a:n-able:n-central:*:*:*:*:*:*	-
N-able N-central Authentication Bypass Using an Alternate Path or Channel Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-288	T1190: Exploit Public-Facing Application	https://status.n-able.com/2026/08/06/n-central-2026-3-hotfix-2-additional-mitigation-for-cve-2026-18577/

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2026-34486		Apache Tomcat: 11.0.20, 10.1.53, 9.0.116	knaithe (aka KnYuan)
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS	cpe:2.3:a:apache:tomcat:*:*:*:*:*:*	SNOWLIGHT
Apache Tomcat Missing Encryption of Sensitive Data Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-311	T1190: Exploit Public-Facing Application	https://tomcat.apache.org/index.html

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2026-9198		IBM Langflow OSS 1.0.0 through 1.10.0	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS	cpe:2.3:a:langflow:langflow:*:*:*:*:*:*	-
IBM Langflow Code Injection Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-94	T1190: Exploit Public-Facing Application, T1059.006: Command and Scripting Interpreter: Python	https://www.ibm.com/support/pages/node/7278927

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
<u>CVE-2026-18577</u>		N-able N-central (Before 2026.3.1.7)	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS	cpe:2.3:a:n-able:n-central:*:*:*:*:*:*	-
N-able N-central Authentication Bypass Using an Alternate Path or Channel Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-288	T1190: Exploit Public-Facing Application, T1057: Process Discovery	https://status.n-able.com/2026/08/06/n-central-2026-3-hotfix-2-additional-mitigation-for-cve-2026-18577/

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

September 02, 2026 • 03:50 AM

© 2026 All Rights are Reserved by Hive Pro



More at www.hivepro.com