

Date of Publication
April 3, 2025



HiveForce Labs

CISA

KNOWN

EXPLOITED

VULNERABILITY

CATALOG

March 2025

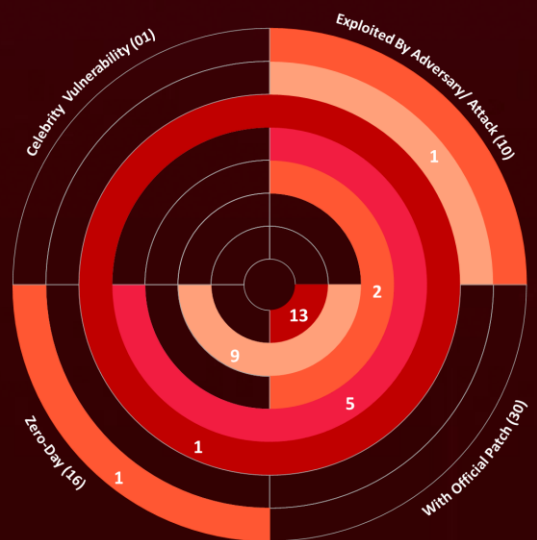
Table of Contents

<u>Summary</u>	03
<u>CVEs List</u>	04
<u>CVEs Details</u>	08
<u>Recommendations</u>	29
<u>References</u>	30
<u>Appendix</u>	30
<u>What Next?</u>	31

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 March 2025, thirty-two vulnerabilities met the criteria for inclusion in the CISA's KEV catalog. Of these, sixteen are zero-day vulnerabilities; ten have been exploited by known threat actors and employed in attacks.






CVEs List




CVE	NAME	AFFECTED PRODUCT	CVSS 3.x SCORE	ZERO-DAY	PATCH	DUE DATE
CVE-2024-20439	Cisco Smart Licensing Utility Static Credential Vulnerability	Cisco Smart Licensing Utility	9.8			April 21, 2025
CVE-2025-2783	Google Chromium Mojo Sandbox Escape Vulnerability	Google Chromium Mojo	8.3			April 17, 2025
CVE-2019-9875	Sitecore CMS and Experience Platform (XP) Deserialization Vulnerability	Sitecore CMS and Experience Platform (XP)	8.8			April 16, 2025
CVE-2019-9874	Sitecore CMS and Experience Platform (XP) Deserialization Vulnerability	Sitecore CMS and Experience Platform (XP)	9.8			April 16, 2025
CVE-2025-30154	reviewdog/action-setup GitHub Action Embedded Malicious Code Vulnerability	Reviewdog action-setup GitHub Action	8.6			April 14, 2025
CVE-2017-12637	SAP NetWeaver Directory Traversal Vulnerability	SAP NetWeaver	7.5			April 9, 2025
CVE-2024-48248	NAKIVO Backup and Replication Absolute Path Traversal Vulnerability	NAKIVO Backup and Replication	8.6			April 9, 2025
CVE-2025-1316	Edimax IC-7100 IP Camera OS Command Injection Vulnerability	Edimax IC-7100 IP Camera	9.8		EOL	April 9, 2025
CVE-2025-30066	tj-actions/changed-files GitHub Action Embedded Malicious Code Vulnerability	tj-actions changed-files GitHub Action	8.6			April 8, 2025
CVE-2025-24472	Fortinet FortiOS and FortiProxy Authentication Bypass Vulnerability	Fortinet FortiOS and FortiProxy	9.8			April 8, 2025




CVE	NAME	AFFECTED PRODUCT	CVSS 3.x SCORE	ZERO-DAY	PATCH	DUE DATE
CVE-2025-21590	Juniper Junos OS Improper Isolation or Compartmentalization Vulnerability	Juniper Junos OS	4.4			April 3, 2025
CVE-2025-24201	Apple Multiple Products WebKit Out-Of-Bounds Write Vulnerability	Apple Multiple Products	8.8			April 3, 2025
CVE-2025-24993	Microsoft Windows NTFS Heap-Based Buffer Overflow Vulnerability	Microsoft Windows	7.8			April 1, 2025
CVE-2025-24991	Microsoft Windows NTFS Out-Of-Bounds Read Vulnerability	Microsoft Windows	5.5			April 1, 2025
CVE-2025-24985	Microsoft Windows Fast FAT File System Driver Integer Overflow Vulnerability	Microsoft Windows	7.8			April 1, 2025
CVE-2025-24984	Microsoft Windows NTFS Information Disclosure Vulnerability	Microsoft Windows	4.6			April 1, 2025
CVE-2025-24983	Microsoft Windows Win32k Use-After-Free Vulnerability	Microsoft Windows	7.0			April 1, 2025
CVE-2025-26633	MSC EvilTwin (Microsoft Windows Management Console (MMC) Improper Neutralization Vulnerability)	Microsoft Windows	7.0			April 1, 2025
CVE-2024-13161	Ivanti Endpoint Manager (EPM) Absolute Path Traversal Vulnerability	Ivanti Endpoint Manager (EPM)	7.5			March 31, 2025
CVE-2024-13160	Ivanti Endpoint Manager (EPM) Absolute Path Traversal Vulnerability	Ivanti Endpoint Manager (EPM)	7.5			March 31, 2025




CVE	NAME	AFFECTED PRODUCT	CVSS 3.x SCORE	ZERO-DAY	PATCH	DUE DATE
CVE-2024-13159	Ivanti Endpoint Manager (EPM) Absolute Path Traversal Vulnerability	Ivanti Endpoint Manager (EPM)	7.5			March 31, 2025
CVE-2024-57968	Advantive VeraCore Unrestricted File Upload Vulnerability	Advantive VeraCore	8.8			March 31, 2025
CVE-2025-25181	Advantive VeraCore SQL Injection Vulnerability	Advantive VeraCore	7.5			March 31, 2025
CVE-2025-22226	VMware ESXi, Workstation, and Fusion Information Disclosure Vulnerability	Vmware ESXi, Workstation, and Fusion	6.0			March 25, 2025
CVE-2025-22225	VMware ESXi Arbitrary Write Vulnerability	Vmware ESXi	8.2			March 25, 2025
CVE-2025-22224	VMware ESXi and Workstation TOCTOU Race Condition Vulnerability	Vmware ESXi and Workstation	8.2			March 25, 2025
CVE-2024-50302	Linux Kernel Use of Uninitialized Resource Vulnerability	Linux Kernel	5.5			March 25, 2025
CVE-2024-4885	Progress WhatsUp Gold Path Traversal Vulnerability	Progress WhatsUp Gold	9.8			March 24, 2025
CVE-2018-8639	Microsoft Windows Win32k Improper Resource Shutdown or Release Vulnerability	Microsoft Windows	7.8			March 24, 2025
CVE-2022-43769	Hitachi Vantara Pentaho BA Server Special Element Injection Vulnerability	Hitachi Vantara Pentaho Business Analytics (BA) Server	7.2			March 24, 2025
CVE-2022-43939	Hitachi Vantara Pentaho BA Server Authorization Bypass Vulnerability	Hitachi Vantara Pentaho Business Analytics (BA) Server	9.8			March 24, 2025

CVE	NAME	AFFECTED PRODUCT	CVSS 3.x SCORE	ZERO-DAY	PATCH	DUE DATE
CVE-2023-20118	Cisco Small Business RV Series Routers Command Injection Vulnerability	Cisco Small Business RV Series Routers	7.2		EOL	March 24, 2025

CVEs Details




CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2024-20439		Cisco Smart Licensing Utility versions 2.0.0, 2.1.0, and 2.2.0	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS	cpe:2.3:a:cisco:smart_license_utility:*:*:*:*:*	-
Cisco Smart Licensing Utility Static Credential Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-912	T1068: Exploitation for Privilege Escalation, T1552.001: Credentials In Files	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-cslu-7gHMzWmw

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2025-2783		Google Chrome (Windows) Version prior to 134.0.6998.178	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS	cpe:2.3:a:google:chrome:*:* :*:*:*:*	-
Google Chromium Mojo Sandbox Escape Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-20	T1059: Command and Scripting Interpreter; T1497: Virtualization/Sandbox Evasion; T1036: Masquerading	https://chromereleases.googleblog.com/2025/03/stable-channel-update-for-desktop_25.html




CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2019-9875		Sitecore Version Prior to 9.1.0	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS	cpe:2.3:a:sitecore:cms:*:* :*:*:*:*	-
Sitecore CMS and Experience Platform (XP) Deserialization Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-502	T1059: Command and Scripting Interpreter	https://developers.sitecore.com/Downloads




CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2019-9874		Sitecore CMS Version 7.0 to 7.2 and Sitecore XP Version 7.5 to 8.2	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS	cpe:2.3:a:sitecore:cms:*:*:*:*:*:*	
Sitecore CMS and Experience Platform (XP) Deserialization Vulnerability		cpe:2.3:a:sitecore:experience_platform:*:*:*:*:*:*	-
	CWE ID	ASSOCIATED TTPs	PATCH LINKS
	CWE-502	T1059: Command and Scripting Interpreter	https://developers.sitecore.com/Downloads




CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
<u>CVE-2025-30154</u>		reviewdog/action-setup@v1	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS	cpe:2.3:a:reviewdog:action-setup:*:*:*:*:*:*	
reviewdog/action-setup GitHub Action Embedded Malicious Code Vulnerability			-
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-506	T1055: Process Injection	https://github.com/reviewdog/action-setup/releases/tag/v1.3.2




CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2017-12637		SAP NetWeaver Application Server Java Version 7.5	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS	cpe:2.3:a:sap:netweaver_application_server_java:7.50:*:*:*:*:*:*	-
SAP NetWeaver Directory Traversal Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINKS
	CWE-22	T1202: Indirect Command Execution	https://me.sap.com/notes/3476549




CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2024-48248		NAKIVO Backup & Replication before 11.0.0.88174	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS	cpe:2.3:a:nakivo:backup_&_replication_director:*:*:*:*:*:*	-
NAKIVO Backup and Replication Absolute Path Traversal Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-36	T1059: Command and Scripting Interpreter	https://helpcenter.nakivo.com/Release-Notes/Content/Release-Notes.htm




CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2025-1316		Edimax IC-7100 IP Camera All versions	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS	cpe:2.3:o:edimax:ic-7100_firmware:*:*:*:*:*:*:*	Mirai Botnet
Edimax IC-7100 IP Camera OS Command Injection Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINKS
	CWE-78	T1059: Command and Scripting Interpreter, T1566: Phishing, T1203: Exploitation for Client Execution	EOL




CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2025-30066		GitHub Action v1 through v45.0.7	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS	cpe:2.3:a:tj-actions:changed-files:*:*:*:*:*:*	-
tj-actions/changed-files GitHub Action Embedded Malicious Code Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-506	T1195: Supply Chain Compromise; T1055: Process Injection	https://github.com/tj-actions/changed-files/releases/tag/v46.0.1




CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
<u>CVE-2025-24472</u>		Fortinet FortiOS and FortiProxy Office	Mora_001
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS	cpe:2.3:o:fortinet:fortios: *.*.*.*.*.*.*	SuperBlack
Fortinet FortiOS Authorization Bypass Vulnerability		cpe:2.3:a:fortinet:fortiproxy: *.*.*.*.*.*.* cpe:2.3:a:fortinet:fortios: *.*.*.*.*.*.*	
	CWE ID	ASSOCIATED TTPs	
	CWE-288	T1059: Command and Scripting Interpreter; T1068: Exploitation for Privilege Escalation	https://fortiguard.fortinet.com/psirt/FG-IR-24-535




CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2025-21590		Junos OS: All versions before 21.2R3-S9, 21.4 versions before 21.4R3 S10, 22.2 versions before 22.2R3-S6, 22.4 versions before 22.4R3-S6, 23.2 versions before 23.2R2-S3, 23.4 versions before 23.4R2-S4, 24.2 versions before 24.2R1-S2, 24.2R2.	UNC3886
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS	cpe:2.3:o:juniper:junos:*:*:*:*:*	-
Juniper Junos OS Improper Isolation or Compartmentalization Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-653	T1059: Command and Scripting Interpreter	https://supportportal.juniper.net/s/article/2025-03-Out-of-Cycle-Security-Bulletin-Junos-OS-A-local-attacker-with-shell-access-can-execute-arbitrary-code-CVE-2025-21590?language=en_US




CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
<u>CVE-2025-24201</u>		Apple iOS and iPadOS Versions before 18.3.2, Apple macOS Sequoia Versions before 15.3.2, Apple visionOS Version before 2.3.2, Apple Safari Version before 18.3.1	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS	cpe:2.3:a:apple:visionos:*:*:*:*:*:* cpe:2.3:a:apple:safari:*:*:*:*:*:* cpe:2.3:a:apple:macos_sequoia:*:*:*:*:*:* cpe:2.3:a:apple:ios:*:*:*:*:*:*	-
Apple Multiple Products WebKit Out-of-Bounds Write Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINKS
	CWE-787	T1497: Virtualization/Sandbox Evasion; T1190: Exploit Public-Facing Application	https://support.apple.com/en-us/118481 , https://support.apple.com/en-us/118575 , https://support.apple.com/en-us/108382 , https://support.apple.com/en-us/122285



CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2025-24993		Windows: 10 - 11 24H2 Windows Server: 2008 - 2025	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS	cpe:2.3:o:microsoft:windows:*:*:*:*:*:* cpe:2.3:o:microsoft:windows_server:*:*:*:*:*:*	
Microsoft Windows NTFS Heap-Based Buffer Overflow Vulnerability			-
	CWE ID	ASSOCIATED TTPs	PATCH LINKS
	CWE-122	T1059: Command and Scripting Interpreter	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-24993

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2025-24991		Windows: 10 - 11 24H2 Windows Server: 2008 - 2025	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS	cpe:2.3:o:microsoft:windows:*:*:*:*:*:* cpe:2.3:o:microsoft:windows_server:*:*:*:*:*:*	
Microsoft Windows NTFS Out-Of-Bounds Read Vulnerability			-
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-125	T1588.006: Vulnerabilities; T1068: Exploitation for Privilege Escalation	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-24991

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2025-24985		Windows: 10 - 11 24H2 Windows Server: 2008 - 2025	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS	cpe:2.3:o:microsoft:windows:*:*:*:*:*:* cpe:2.3:o:microsoft:windows_server:*:*:*:*:*:*	
Windows Fast FAT File System Driver Remote Code Execution Vulnerability			-
	CWE ID	ASSOCIATED TTPs	PATCH LINKS
	CWE-190 CWE-122	T1059: Command and Scripting Interpreter	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-24985




CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2025-24984		Windows: 10 - 11 24H2 Windows Server: 2012 - 2025	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS	cpe:2.3:o:microsoft:windows:*:*:*:*:*:* cpe:2.3:o:microsoft:windows_server:*:*:*:*:*:*	
Windows NTFS Information Disclosure Vulnerability			-
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-532	T1588.006: Vulnerabilities; T1068: Exploitation for Privilege Escalation	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-24984




CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2025-24983		Windows: 10 Windows Server: 2008 - 2016	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS	cpe:2.3:o:microsoft:windows:*:*:*:*:*:* cpe:2.3:o:microsoft:windows_server:*:*:*:*:*:*	
Windows Win32 Kernel Subsystem Elevation of Privilege Vulnerability			-
	CWE ID	ASSOCIATED TTPs	PATCH LINKS
	CWE-416	T1068: Exploitation for Privilege Escalation	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-24983




CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2025-26633	MSC EvilTwin	Windows: 10 - 11 24H2 Windows Server: 2008 - 2025	Water Gamayun
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS	cpe:2.3:o:microsoft:windows:*:*:*:*:*:* cpe:2.3:o:microsoft:windows_server:*:*:*:*:*:*	EncryptHub stealer, DarkWisp backdoor, SilentPrism backdoor, Rhadamanthys, Stealc, and MSC EvilTwin loader
Microsoft Management Console Security Feature Bypass Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-707	T1553: Subvert Trust Controls; T1204: User Execution; T1566: Phishing	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-26633




CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2024-13161		Endpoint Manager Version before 2022 SU6 January-2025 Update	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS	cpe:2.3:a:ivanti:endpoint_manager:*:*:*:*:*:*	-
Ivanti Endpoint Manager (EPM) Absolute Path Traversal Vulnerability			
	CWE ID	T1068: Exploitation for Privilege Escalation	https://forums.ivanti.com/s/article/Security-Advisory-EPM-January-2025-for-EPM-2024-and-EPM-2022-SU6?language=en_US
	CWE-36		




CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2024-13160		Endpoint Manager Version before 2022 SU6 January-2025 Update	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS	cpe:2.3:a:ivanti:endpoint_manager:*:*:*:*:*:*	-
Ivanti Endpoint Manager (EPM) Absolute Path Traversal Vulnerability			
	CWE ID	T1068: Exploitation for Privilege Escalation	https://forums.ivanti.com/s/article/Security-Advisory-EPM-January-2025-for-EPM-2024-and-EPM-2022-SU6?language=en_US
	CWE-36		



CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2024-13159		Endpoint Manager Version before 2022 SU6 January-2025 Update	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS	cpe:2.3:a:ivanti:endpoint_manager:*:*:*:*:*:*	-
Ivanti Endpoint Manager (EPM) Absolute Path Traversal Vulnerability			
	CWE-36	T1068: Exploitation for Privilege Escalation	PATCH LINKS




CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2024-57968		Advantive VeraCore Version before 2024.4.2.1	XE Group
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS	cpe:2.3:a:advantive:veracore:*:*:*:*:*:*	ASPXSpy
Advantive VeraCore Unrestricted File Upload Vulnerability			
	CWE-434	T1190: Exploit Public-Facing Application	PATCH LINK




CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2025-25181		Advantive VeraCore through 2025.1.0	XE Group
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS	cpe:2.3:a:advantive:veracore:*:*:*:*:*:*	ASPXSpy
Advantive VeraCore SQL Injection Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINKS
	CWE-89	T1059: Command and Scripting Interpreter, T1190: Exploit Public-Facing Application	https://advantive.my.site.com/support/s/article/Veracore-Release-Notes-2025-1-1-3




CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
<u>CVE-2025-22226</u>		VMware ESXi Versions 7.0 and 8.0, VMware Cloud Foundation Version 4.5.x and 5.x, VMware Telco Cloud Platform Version 5.x, 4.x, 3.x, and 2.x, VMware Telco Cloud Infrastructure Version 3.x and 2.x, VMware Workstation Version 17.x, VMware Fusion Version 13.x	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS	cpe:2.3:o:vmware:esxi:-:*:*:*:*:*:* cpe:2.3:a:vmware:cloud_foundation:*:*:*:*:*:* cpe:2.3:a:vmware:telco_cloud_platform:*:*:*:*:*:* cpe:2.3:a:vmware:workstation:*:*:*:*:*:* cpe:2.3:a:vmware:fusion:*:*:*:*:*:*	
VMware ESXi, Workstation, and Fusion Information Disclosure Vulnerability			-
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-125	T1059: Command and Scripting Interpreter, T1068: Exploitation for Privilege Escalation	https://support.broadcom.com/web/ecx/support-content-notification/-/external/content/SecurityAdvisories/0/25390




CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
<u>CVE-2025-22225</u>		VMware ESXi Versions 7.0 and 8.0, VMware Cloud Foundation Version 4.5.x and 5.x, VMware Telco Cloud Platform Version 5.x, 4.x, 3.x, and 2.x, VMware Telco Cloud Infrastructure Version 3.x and 2.x	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS	cpe:2.3:a:vmware:cloud_foundation:*:*:*:*:*:*:*:* *:*:* cpe:2.3:a:vmware:telco_cloud_platform:*:*:*:*:*:*:*:* *:*	-
VMware ESXi Arbitrary Write Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINKS
	CWE-123	T1059: Command and Scripting Interpreter, T1068: Exploitation for Privilege Escalation	https://support.broadcom.com/web/ecx/support-content-notification/-/external/content/SecurityAdvisories/0/25390




CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
<u>CVE-2025-22224</u>		VMware ESXi Versions 7.0 and 8.0, VMware Cloud Foundation Version 4.5.x and 5.x, VMware Telco Cloud Platform Version 5.x, 4.x, 3.x, and 2.x, VMware Telco Cloud Infrastructure Version 3.x and 2.x, VMware Workstation Version 17.x	APT28 (aka Fancy Bear), APT29 (aka Cozy Bear), and APT41
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS	cpe:2.3:o:vmware:esxi:- .*:.*:.*:.*:.*:.* cpe:2.3:a:vmware:cloud_foundation:.*:.*:.*:.*:.*:.* .*:.* cpe:2.3:a:vmware:telco_cloud_platform:.*:.*:.*:.*:.*:.* .*:.* cpe:2.3:a:vmware:workstation:.*:.*:.*:.*:.*:.*	
VMware ESXi and Workstation TOCTOU Race Condition Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINKS
	CWE-367	T1059: Command and Scripting Interpreter, T1068 : Exploitation for Privilege Escalation	https://support.broadcom.com/web/ecx/support-content-notification/-/external/content/SecurityAdvisories/0/25390




CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2024-50302		Linux Kernels before 5.4.286, Kernels before 4.19.324, Kernels before 5.10.230, Kernels before 5.15.172, Kernels before 6.1.117, Kernels before 6.6.61, Kernels before 6.11.8	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS	cpe:2.3:o:linux:linux_kernel:*:*:*:*:*:*	NoviSpy
Linux Kernel Use of Uninitialized Resource Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINKS
	CWE-908	T1499: Endpoint Denial of Service	https://web.git.kernel.org/pub/scm/linux/kernel/git/stable/linux.git/commit/?id=d7dc68d82ab3fcfc3f65322465da3d7031d4ab46

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2024-4885		WhatsUp Gold versions released before 2023.1.3	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS	cpe:2.3:a:progress:whatsup_gold:*:*:*:*:*:*	-
Progress WhatsUp Gold Path Traversal Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-22	T1059: Command and Scripting Interpreter, T1608.001: Upload Malware	https://community.progress.com/s/article/WhatsUp-Gold-Security-Bulletin-June-2024

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2018-8639		Windows 7, Windows Server 2012 R2, Windows RT 8.1, Windows Server 2008, Windows Server 2019, Windows Server 2012, Windows 8.1, Windows Server 2016, Windows Server 2008 R2, Windows 10, Windows 10 Servers	Dalbit (aka m00nlight)
	ZERO-DAY		
		AFFECTED CPE	
NAME	BAS ATTACKS	cpe:2.3:o:microsoft:windows:*:*:*:*:*	-
Microsoft Windows Win32k Improper Resource Shutdown or Release Vulnerability			ASSOCIATED TTPs
	CWE ID		
	CWE-404	T1068: Exploitation for Privilege Escalation, T1136: Create Account	https://msrc.microsoft.com/update-guide/en-US/advisory/CVE-2018-8639

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2022-43769		Hitachi Vantara Pentaho Business Analytics Server prior to versions 9.4.0.1 and 9.3.0.2, including 8.3.x	-
	ZERO-DAY		
		AFFECTED CPE	
NAME	BAS ATTACKS	cpe:2.3:a:hitachi:vantara_pentaho_business_analytics_server:*:*:*:*:*	-
Hitachi Vantara Pentaho BA Server Special Element Injection Vulnerability			ASSOCIATED TTPs
	CWE ID		
	CWE-94 CWE-74	T1059: Command and Scripting Interpreter	https://docs.hitachivantara.com/r/en-us/pentaho-data-integration-and-analytics/9.4.x/mk-95pdia000/install-the-30-day-trial-of-pentaho-data-integration-and-analytics/download-the-software

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2022-43939		Hitachi Vantara Pentaho Business Analytics Server versions before 9.4.0.1 and 9.3.0.2	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS	cpe:2.3:a:hitachi:vantara_pentaho_business_analytics_server:*.~*~*~*~*~*~*	-
Hitachi Vantara Pentaho BA Server Authorization Bypass Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINKS
	CWE-647	T1556: Modify Authentication Process, T1068: Exploitation for Privilege Escalation	https://support.pentaho.com/hc/en-us/articles/14455394120333--Resolved-Pentaho-BA-Server-Use-of-Non-Canonical-URL-Paths-for-Authorization-Decisions-Versions-before-9-4-0-1-and-9-3-0-2-including-8-3-x-Impacted-CVE-2022-43939

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2023-20118		Cisco Small Business RV Series Routers	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS	cpe:2.3:o:cisco:rv016_firmware:*: *:*:*:*:*:* cpe:2.3:h:cisco:rv016:-:*:*:*:*:*:* cpe:2.3:o:cisco:rv042_firmware:*: *:*:*:*:*:* cpe:2.3:h:cisco:rv042:-:*:*:*:*:*:* cpe:2.3:o:cisco:rv042g_firmware:*: *:*:*:*:*:* cpe:2.3:h:cisco:rv042g:-:*:*:*:*:*:* cpe:2.3:o:cisco:rv082_firmware:*: *:*:*:*:*:* cpe:2.3:h:cisco:rv082:-:*:*:*:*:*:* cpe:2.3:o:cisco:rv320_firmware:*: *:*:*:*:*:* cpe:2.3:h:cisco:rv320:-:*:*:*:*:*:* cpe:2.3:o:cisco:rv325_firmware:*: *:*:*:*:*:* cpe:2.3:h:cisco:rv325:-:*:*:*:*:*:*	PolarEdge Botnet
			
Cisco Small Business RV Series Routers Command Injection Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINKS
	CWE-77	T1059: Command and Scripting Interpreter	EOL

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 22-01 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.

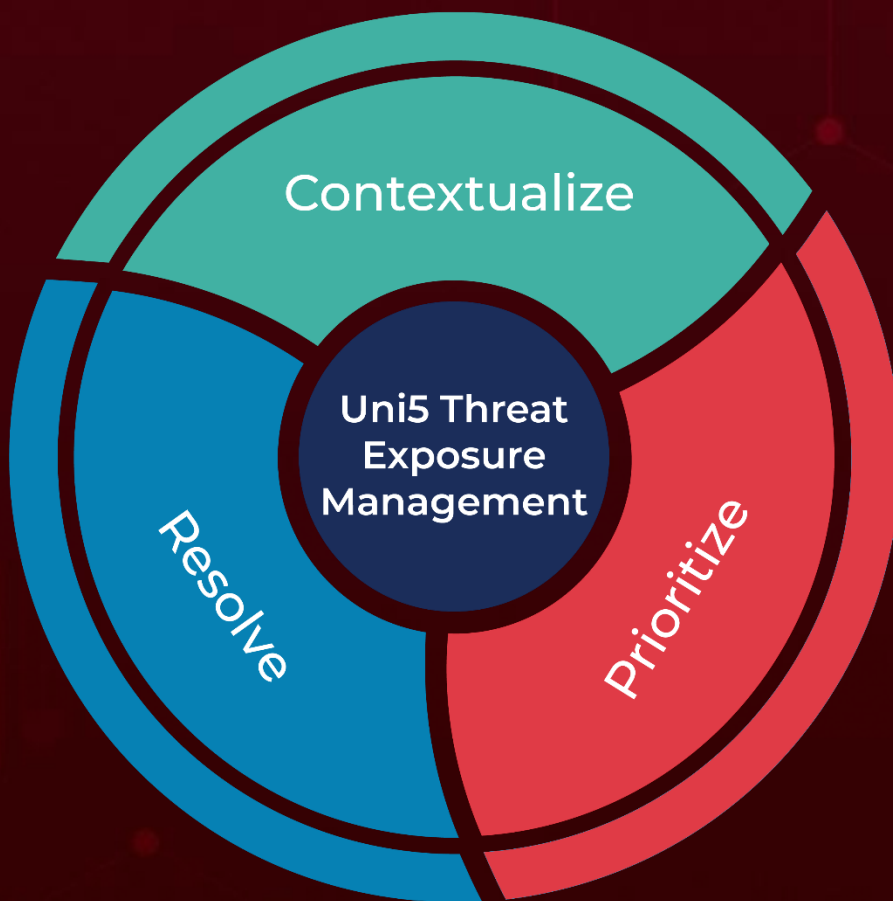
BAS Attacks: “BAS attacks” are the simulated cyber-attacks that can be carried out by our in-house Uni5's Breach and Attack Simulation (BAS), which organizations could use to identify vulnerabilities and improve their overall security posture.

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 free demo with HivePro Uni5:Threat Exposure Management Platform.



REPORT GENERATED ON

April 3, 2025 • 7:00 AM

© 2025 All Rights are Reserved by Hive Pro



More at www.hivepro.com