

Date of Publication
February 4, 2025



HiveForce Labs

CISA

KNOWN

EXPLOITED

VULNERABILITY

CATALOG

January 2025

Table of Contents

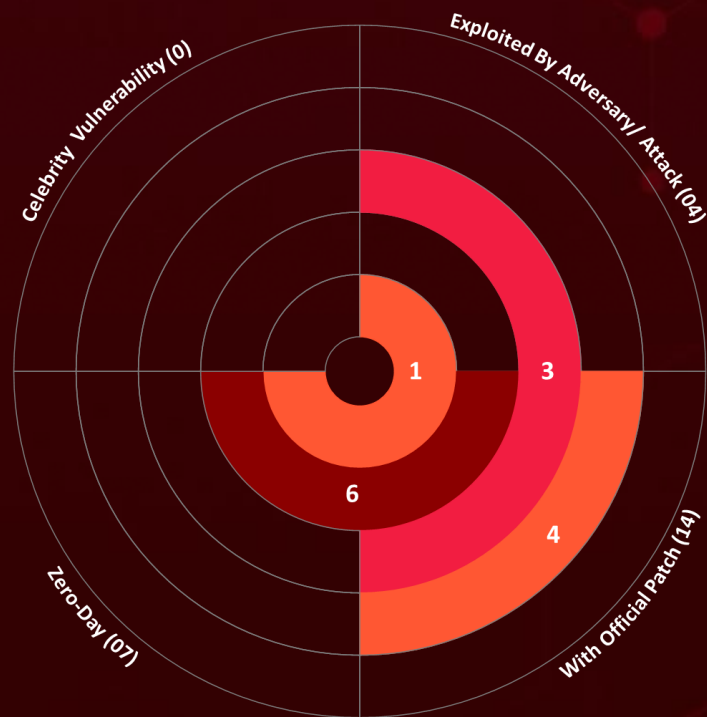
<u>Summary</u>	03
<u>CVEs List</u>	04
<u>CVEs Details</u>	06
<u>Recommendations</u>	14
<u>References</u>	15
<u>Appendix</u>	15
<u>What Next?</u>	16

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 January 2025, **fourteen** vulnerabilities met the criteria for inclusion in the CISA's KEV catalog. Of these, **seven** are **zero-day** vulnerabilities; **four** have been **exploited** by known threat actors and employed in attacks.











14
Known Exploited
Vulnerabilities











CVEs List




CVE	NAME	AFFECTED PRODUCT	CVSS 3.x SCORE	ZERO-DAY	PATCH	DUE DATE
CVE-2025-24085	Apple Multiple Products Use-After-Free Vulnerability	Apple Multiple Products	7.8	✓	✓	February 19, 2025
CVE-2025-23006	SonicWall SMA1000 Appliances Deserialization Vulnerability	SonicWall SMA1000 Appliances	9.8	✓	✓	February 14, 2025
CVE-2020-11023	JQuery Cross-Site Scripting (XSS) Vulnerability	Jquery	6.1	✗	✓	February 13, 2025
CVE-2024-50603	Aviatrix Controllers OS Command Injection Vulnerability	Aviatrix Controllers	9.8	✗	✓	February 6, 2025
CVE-2025-21335	Microsoft Windows Hyper-V NT Kernel Integration VSP Use-After-Free Vulnerability	Microsoft Windows	7.8	✓	✓	February 4, 2025
CVE-2025-21334	Microsoft Windows Hyper-V NT Kernel Integration VSP Use-After-Free Vulnerability	Microsoft Windows	7.8	✓	✓	February 4, 2025
CVE-2025-21333	Microsoft Windows Hyper-V NT Kernel Integration VSP Heap-based Buffer Overflow Vulnerability	Microsoft Windows	7.8	✓	✓	February 4, 2025
CVE-2024-55591	Fortinet FortiOS and FortiProxy Authentication Bypass Vulnerability	Fortinet FortiOS and FortiProxy	9.8	✓	✓	January 21, 2025
CVE-2023-48365	Qlik Sense HTTP Tunneling Vulnerability	Qlik Sense	9.9	✗	✓	February 3, 2025




CVE	NAME	AFFECTED PRODUCT	CVSS 3.x SCORE	ZERO-DAY	PATCH	DUE DATE
CVE-2024-12686	BeyondTrust Privileged Remote Access (PRA) and Remote Support (RS) OS Command Injection Vulnerability	BeyondTrust Privileged Remote Access (PRA) and Remote Support (RS)	7.2			February 3, 2025
CVE-2025-0282	Ivanti Connect Secure, Policy Secure, and ZTA Gateways Stack-Based Buffer Overflow Vulnerability	Ivanti Connect Secure, Policy Secure, and ZTA Gateways	9.0			January 15, 2025
CVE-2020-2883	Oracle WebLogic Server Unspecified Vulnerability	Oracle WebLogic Server	9.8			January 28, 2025
CVE-2024-55550	Mitel MiCollab Path Traversal Vulnerability	Mitel MiCollab	2.7			January 28, 2025
CVE-2024-41713	Mitel MiCollab Path Traversal Vulnerability	Mitel MiCollab	9.1			January 28, 2025




CVEs Details




CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
<u>CVE-2025-24085</u>		Apple visionOS Version affected before 2.3, tvOS Version affected before 18.3, macOS Version affected before 15.3, watchOS Version affected before 11.3, iOS and iPadOS Version affected before 18.3	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS	cpe:2.3:o:apple:tvos:*:*:*:*:*:*:* cpe:2.3:a:apple:watchos:*:*:*:*:*:* cpe:2.3:a:apple:visionos:*:*:*:*:*:* cpe:2.3:a:apple:macos:*:*:*:*:*:* cpe:2.3:a:apple:ios:*:*:*:*:*:*:*:*	-
Apple Multiple Products Use-After-Free Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINKS
	CWE-416	T1068: Exploitation for Privilege Escalation, T1059: Command and Scripting Interpreter	https://support.apple.com/en-us/122066 https://support.apple.com/en-us/122068 https://support.apple.com/en-us/122071 https://support.apple.com/en-us/122072 https://support.apple.com/en-us/122073




CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
<u>CVE-2025-23006</u>		SonicWall SMA1000 Appliance Management Console (AMC) and Central Management Console (CMC) Version 12.4.3-02804 and earlier	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS	cpe:2.3:h:sonicwall:sma1000:*:*:*:*:*:*	-
SonicWall SMA1000 Appliances Deserialization Vulnerability			
	CWE ID		
	CWE-502	T1059: Command and Scripting Interpreter, T1068: Exploitation for Privilege Escalation	https://www.sonicwall.com/support/knowledge-base/product-notice-urgent-security-notification-sma-1000/250120090802840




CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
<u>CVE-2020-11023</u>		jQuery versions from 1.0.3 and prior 3.5.0	APT1, APT27
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS	cpe:2.3:a:jquery:jquery:*:*:*:*:*:*	-
jQuery Cross-Site Scripting (XSS) Vulnerability			
	CWE ID		
	CWE-79	T1189: Drive-by Compromise, T1204.001: Malicious Link, T1204: User Execution	https://blog.jquery.com/2020/04/10/jquery-3-5-0-released/




CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2024-50603		Aviatrix Controller before 7.1.4191 and 7.2.x before 7.2.4996	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS	cpe:2.3:a:aviatrix:controller:*:*:*:*:*:*	XMRig, Sliver backdoor
Aviatrix Controllers OS Command Injection Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-78	T1059: Command and Scripting Interpreter	https://docs.aviatrix.com/documentation/latest/release-notices/psirt-advisories/psirt-advisories.html




CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2025-21335		Windows: 10 - 11 24H2 Windows Server 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 Hyper-V NT Kernel Integration VSP Use-After-Free Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-416	T1059: Command and Scripting Interpreter, T1068: Exploitation for Privilege Escalation	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-21335




CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
<u>CVE-2025-21334</u>		Windows: 10 - 11 24H2 Windows Server 2025	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS	cpe:2.3:o:microsoft:windows:* :*:*:*:*:*:*	-
Microsoft Windows Hyper-V NT Kernel Integration VSP Use-After-Free Vulnerability		cpe:2.3:o:microsoft:windows_server:*:*:*:*:*:*	-
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-416	T1059: Command and Scripting Interpreter, T1068 : Exploitation for Privilege Escalation	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-21334




CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
<u>CVE-2025-21333</u>		Windows: 10 - 11 24H2 Windows Server: 2022 - 2025	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS	cpe:2.3:o:microsoft:windows:*:*:*:*:*:*	-
Microsoft Windows Hyper-V NT Kernel Integration VSP Heap-based Buffer Overflow Vulnerability		cpe:2.3:o:microsoft:windows_server:*:*:*:*:*:*	-
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-122	T1059: Command and Scripting Interpreter, T1068: Exploitation for Privilege Escalation	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-21333

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR	
CVE-2024-55591		FortiOS Versions 7.0.0 through 7.0.16, FortiProxy Versions 7.2.0 through 7.2.12, FortiProxy Versions 7.0.0 through 7.0.19	-	
	ZERO-DAY			
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE	
NAME	BAS ATTACKS	cpe:2.3:a:fortinet:fortiproxy:*:*:*:*:*:* cpe:2.3:o:fortinet:fortios:*:*:*:*:*:*	-	
Fortinet FortiOS and FortiProxy Authentication Bypass Vulnerability		CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-288			

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR	
CVE-2023-48365		All versions of Qlik Sense Enterprise for Windows prior to August 2023 Patch 2	Magnet Goblin	
	ZERO-DAY			
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE	
NAME	BAS ATTACKS	cpe:2.3:a:qlik:qlik_sense:-:*:*:enterprise:windows:*:*	Cactus ransomware, NerbianRAT, WARPWIRE, MiniNerbian	
Qlik Sense HTTP Tunneling Vulnerability		CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-444			

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2024-12686		BeyondTrust Privileged Remote Access (PRA) 24.3.1 and earlier, Remote Support (RS) 24.3.1 and earlier	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS	cpe:2.3:a:beyondtrust:priviled_remote_access:*:*:*:*:*:*:*	
BeyondTrust Privileged Remote Access (PRA) and Remote Support (RS) OS Command Injection Vulnerability		cpe:2.3:a:beyondtrust:remote_support:*:*:*:*:*:*:*	-
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-78	T1059: Command and Scripting Interpreter, T1133: External Remote Services, T1068: Exploitation for Privilege Escalation	https://www.beyondtrust.com/trust-center/security-advisories/bt24-11

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2020-2883		Oracle WebLogic Server product of Oracle Fusion Middleware versions 10.3.6.0.0, 12.1.3.0.0, 12.2.1.3.0 and 12.2.1.4.0	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS	cpe:2.3:a:oracle:weblogic_server*:*:*:*:*:*:*	
Oracle WebLogic Server Unspecified Vulnerability			-
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-502	T1059: Command and Scripting Interpreter, T1190: Exploit Public-Facing Application	https://www.oracle.com/security-alerts/cpuapr2020.html

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
<u>CVE-2025-0282</u>		Ivanti Connect Secure: 22.7R2 through 22.7R2.4, Ivanti Policy Secure: 22.7R1 through 22.7R1.2, Ivanti Neurons for ZTA gateways: 22.7R2 through 22.7R2.3	CL-UNK-0979, UNC5337
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS	cpe:2.3:a:ivanti:connect_secure:*:*:*:*:*:* cpe:2.3:a:ivanti:policy_secure:*:*:*:*:*:* cpe:2.3:a:ivanti:neurons_for_zta_gateways:*:*:*:*:*:*	DRYHOOK, PHASEJAM, SPAWNANT, SPAWNMOLE, SPAWNSNAIL, SPAWNSLOTH
Ivanti Connect Secure, Policy Secure, and ZTA Gateways Stack-Based Buffer Overflow Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-787 CWE-121	T1059: Command and Scripting Interpreter, T1210: Exploitation of Remote Services	https://forums.ivanti.com/s/article/Security-Advisory-Ivanti-Connect-Secure-Policy-Secure-ZTA-Gateways-CVE-2025-0282-CVE-2025-0283

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2024-55550		MiCollab Version 9.8 SP1 FP2 (9.8.1.201) and earlier	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS	cpe:2.3:a:mitel:micollab:*:*:*:*:*:*:*	-
Mitel MiCollab Path Traversal Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-22	T1078: Valid Accounts	https://www.mitel.com/support/security-advisories/mitel-product-security-advisory-misa-2024-0029

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2024-41713		MiCollab Version 9.8 SP1 FP2 (9.8.1.201) and earlier	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS	cpe:2.3:a:mitel:micollab:*:*:*:*:*:*:*	-
Mitel MiCollab Path Traversal Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-22	T1016: System Network Configuration Discovery	https://www.mitel.com/support/security-advisories/mitel-product-security-advisory-misa-2024-0029

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.

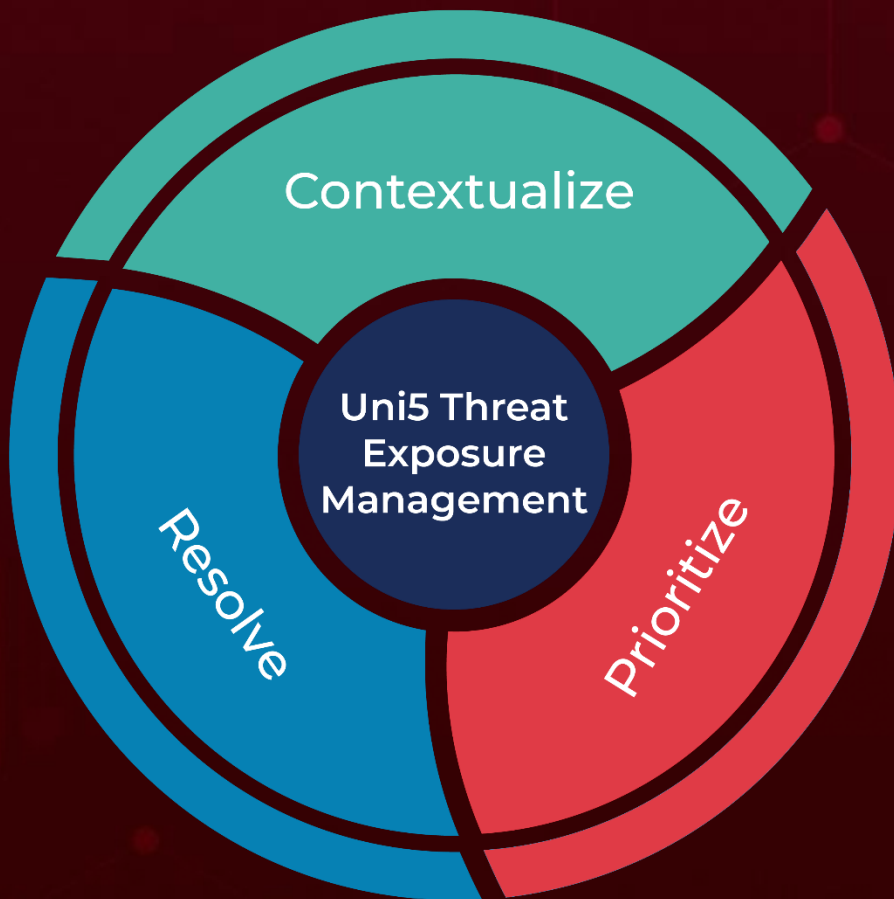
BAS Attacks: “BAS attacks” are the simulated cyber-attacks that can be carried out by our in-house Uni5's Breach and Attack Simulation (BAS), which organizations could use to identify vulnerabilities and improve their overall security posture.

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

February 4, 2025 • 3:30 AM

© 2025 All Rights are Reserved by Hive Pro



More at www.hivepro.com