Date of Publication
December 3, 2024

Hive Pro

HiveForce Labs

CISA KNOWN EXPLOITED VULNERABILITY CATALOG

November 2024

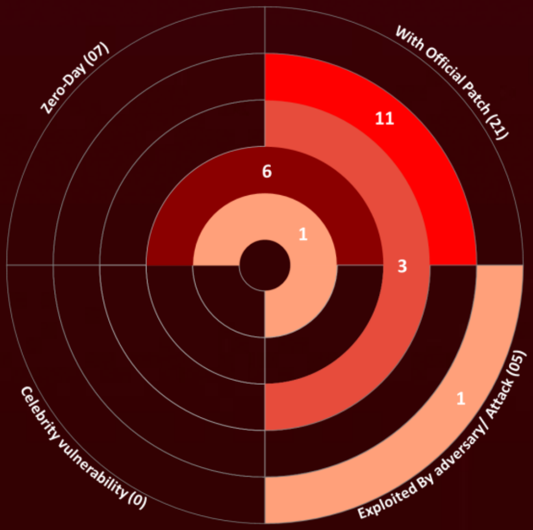
Table of Contents

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 November 2024, **twenty-two** vulnerabilities met the criteria for inclusion in the CISA's KEV catalog. Of these, **seven** are zero-day vulnerabilities, **five** have been exploited by known threat actors and employed in attacks.

22
Known Exploited Vulnerabilities



CVEs List

CVE	NAME	AFFECTED PRODUCT	CVSS 3.x SCORE	ZERO-DAY	PATCH	DUE DATE
CVE-2023-28461	Array Networks AG and vxAG ArrayOS Missing Authentication for Critical Function Vulnerability	Array Networks AG/vxAG ArrayOS	9.8	✗	✓	December 16, 2024
CVE-2024-21287	Oracle Agile Product Lifecycle Management (PLM) Incorrect Authorization Vulnerability	Oracle Agile Product Lifecycle Management (PLM)	7.5	✗	✓	December 12, 2024
CVE-2024-44309	Apple Multiple Products Cross-Site Scripting (XSS) Vulnerability	Apple Multiple Products	6.1	✓	✓	December 12, 2024
CVE-2024-44308	Apple Multiple Products Code Execution Vulnerability	Apple Multiple Products	8.8	✓	✓	December 12, 2024
CVE-2024-38813	VMware vCenter Server Privilege Escalation Vulnerability	VMware vCenter Server	9.8	✗	✓	December 11, 2024
CVE-2024-38812	VMware vCenter Server Heap-Based Buffer Overflow Vulnerability	VMware vCenter Server	9.8	✗	✓	December 11, 2024
CVE-2024-9474	Palo Alto Networks PAN-OS Management Interface OS Command Injection Vulnerability	Palo Alto Networks PAN-OS	6.9	✓	✓	December 9, 2024
CVE-2024-0012	Palo Alto Networks PAN-OS Management Interface Authentication Bypass Vulnerability	Palo Alto Networks PAN-OS	9.3	✓	✓	December 9, 2024
CVE-2024-1212	Progress Kemp LoadMaster OS Command Injection Vulnerability	Progress Kemp LoadMaster	9.8	✗	✓	December 9, 2024
CVE-2024-9465	Palo Alto Networks Expedition SQL Injection Vulnerability	Palo Alto Networks Expedition	9.2	✗	✓	December 5, 2024

CVE	NAME	AFFECTED PRODUCT	CVSS 3.x SCORE	ZERO-DAY	PATCH	DUE DATE
CVE-2024-9463	Palo Alto Networks Expedition OS Command Injection Vulnerability	Palo Alto Networks Expedition	9.9	☒	✓	December 5, 2024
CVE-2021-26086	Atlassian Jira Server and Data Center Path Traversal Vulnerability	Atlassian Jira Server and Data Center	5.3	☒	✓	December 3, 2024
CVE-2014-2120	Cisco Adaptive Security Appliance (ASA) Cross-Site Scripting (XSS) Vulnerability	Cisco Adaptive Security Appliance (ASA)	6.1	☒	☒	December 3, 2024
CVE-2021-41277	Metabase GeoJSON API Local File Inclusion Vulnerability	Metabase Metabase	7.5	☒	✓	December 3, 2024
CVE-2024-43451	Microsoft Windows NTLMv2 Hash Disclosure Spoofing Vulnerability	Microsoft Windows	6.5	✓	✓	December 3, 2024
CVE-2024-49039	Microsoft Windows Task Scheduler Privilege Escalation Vulnerability	Microsoft Windows	8.8	✓	✓	December 3, 2024
CVE-2019-16278	Nostromo nhttpd Directory Traversal Vulnerability	Nostromo nhttpd	9.8	☒	✓	November 28, 2024
CVE-2024-51567	CyberPanel Incorrect Default Permissions Vulnerability	CyberPersons CyberPanel	9.8	✓	✓	November 28, 2024
CVE-2024-43093	Android Framework Privilege Escalation Vulnerability	Android Framework	7.8	☒	✓	November 28, 2024

CVE	NAME	AFFECTED PRODUCT	CVSS 3.x SCORE	ZERO-DAY	PATCH	DUE DATE
CVE-2024-5910	Palo Alto Networks Expedition Missing Authentication Vulnerability	Palo Alto Networks Expedition	9.3	✗	✓	November 28, 2024
CVE-2024-8956	PTZOptics PT30X-SDI/NDI Cameras Authentication Bypass Vulnerability	PTZOptics PT30X-SDI/NDI Cameras	9.1	✗	✓	November 25, 2024
CVE-2024-8957	PTZOptics PT30X-SDI/NDI Cameras OS Command Injection Vulnerability	PTZOptics PT30X-SDI/NDI Cameras	9.8	✗	✓	November 25, 2024

CVEs Details

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2023-28461	✗	Array Networks Array AG Series and vxAG 9.4.0.481 and earlier	Earth Kasha
	ZERO-DAY		
	✗	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS	cpe:2.3:o:arraynetworks:arrayos_ag:*:*:*:*:*:*:*:*	LODEINFO, NOOPDOOR
Array Networks AG and vxAG ArrayOS Missing Authentication for Critical Function Vulnerability	✗		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-306	T1059: Command and Scripting Interpreter	https://support.arraynetworks.net/prx/001/http/supportportal.arraynetworks.net/fieldnotices.html

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2024-21287	✗	Oracle Agile PLM Framework Version 9.3.6	-
	ZERO-DAY		
	✗	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS	cpe:2.3:a:oracle:agile_plm_framework:*:*:*:*:*:*:*:*	Helldown Ransomware
Oracle Agile Product Lifecycle Management (PLM) Incorrect Authorization Vulnerability	✗		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-863	T1565: Data Manipulation, T1068: Exploitation for Privilege Escalation, T1190: Exploit Public-Facing Application	https://support.oracle.com/rs?type=doc&id=3058429.1

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2024-44309	✗	Safari Version Prior to 18.1, macOS Version Prior to 15.1, iOS and iPadOS Version Prior to 18.1, visionOS Version Prior to 2.1	-
	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:*:*:*:*:*:*:*:* cpe:2.3:a:apple:ios:*:*:*:*:*:*:*:*	-
Apple Multiple Products Cross-Site Scripting (XSS) Vulnerability	✗		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-79	T1189: Drive-by Compromise	https://support.apple.com/en-us/118575 https://support.apple.com/en-us/118481 https://support.apple.com/en-us/108382

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2024-44308	✗	Safari Version Prior to 18.1, macOS Version Prior to 15.1, iOS and iPadOS Version Prior to 18.1, visionOS Version Prior to 2.1	-
	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:*:*:*:*:*:*:*:* cpe:2.3:a:apple:ios:*:*:*:*:*:*:*:*	-
Apple Multiple Products Code Execution Vulnerability	✗		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-20	T1059: Command and Scripting Interpreter	https://support.apple.com/en-us/118575 https://support.apple.com/en-us/118481 https://support.apple.com/en-us/108382

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2024-38813	❌	VMware vCenter Server: 7.0 - 8.0, VMware Cloud Foundation: 4.x - 5.1.x	-
	ZERO-DAY		
	❌	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS	cpe:2.3:a:vmware:vcenter_server:*:*:*:*:*:*:*:* cpe:2.3:a:vmware:cloud_foundation:*:*:*:*:*:*:*:*	-
VMware vCenter Server Privilege Escalation Vulnerability	❌		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-78	T1068: Exploitation for Privilege Escalation	https://support.broadcom.com/web/ecx/support-content-notification/-/external/content/SecurityAdvisories/0/24968

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2024-38812	❌	VMware vCenter Server: 7.0 - 8.0, VMware Cloud Foundation: 4.x - 5.1.x	-
	ZERO-DAY		
	❌	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS	cpe:2.3:a:vmware:vcenter_server:*:*:*:*:*:*:*:* cpe:2.3:a:vmware:cloud_foundation:*:*:*:*:*:*:*:*	-
VMware vCenter Server Heap-Overflow Vulnerability	❌		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-122	T1574: Hijack Execution Flow, T1021.003: Distributed Component Object Model	https://support.broadcom.com/web/ecx/support-content-notification/-/external/content/SecurityAdvisories/0/24968

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2024-0012	✗	Palo Alto Networks PAN-OS Versions Prior to 11.2.4-h1, Versions Prior to 11.1.5-h1, Versions Prior to 11.0.6-h1, Versions Prior to 10.2.12-h2	-
	ZERO-DAY		
	✓	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS	cpe:2.3:o:paloaltonetworks:pan-os:*:*:*:*:*:*:*:*	-
Palo Alto Networks PAN-OS Management Interface Authentication Bypass Vulnerability	✗		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-306	T1556: Modify Authentication Process	https://security.paloaltonetworks.com/CVE-2024-0012

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2024-9474	✗	Palo Alto Networks PAN-OS Versions Prior to 11.2.4-h1, Versions Prior to 11.1.5-h1, Versions Prior to 11.0.6-h1, Versions Prior to 10.2.12-h2, Versions Prior to 10.1.14-h6	-
	ZERO-DAY		
	✓	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS	cpe:2.3:o:paloaltonetworks:pan-os:*:*:*:*:*:*:*:*	-
Palo Alto Networks PAN-OS Management Interface OS Command Injection Vulnerability	✗		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-78	T1059: Command and Scripting Interpreter	https://security.paloaltonetworks.com/CVE-2024-9474

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2024-1212	✗	Progress Kemp LoadMaster	-
	ZERO-DAY		
	✗	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS	cpe:2.3:a:progress:loadmaster:*:*:*:*:*:*:*:*	-
Progress Kemp LoadMaster OS Command Injection Vulnerability	✓		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-78	T1059: Command and Scripting Interpreter	https://community.progress.com/s/news/MCJVBKIIOYKJCM3MKXNPN7YCM4FE

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2024-9465	✗	Palo Alto Networks’ Expedition versions prior to 1.2.92	-
	ZERO-DAY		
	✗	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS	cpe:2.3:a:paloaltonetworks:expedition:*:*:*:*:*:*:*:*	-
Palo Alto Networks Expedition SQL Injection Vulnerability	✗		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-89	T1059: Command and Scripting Interpreter	https://live.paloaltonetworks.com/t5/expedition-release-notes/expedition-1-2-96-hotfix-information/ta-p/599340

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2024-9463	☒	Palo Alto Networks’ Expedition versions prior to 1.2.92	-
	ZERO-DAY		
	☒	**AFFECTED CPE**	**ASSOCIATED ATTACKS/RANSOMWARE**
NAME	**BAS ATTACKS**	cpe:2.3:a:paloaltonetworks:expedition:*:*:*:*:*:*:*:*	-
Palo Alto Networks Expedition OS Command Injection Vulnerability	☒		
	CWE ID	**ASSOCIATED TTPs**	**PATCH LINK**
	CWE-78	T1059: Command and Scripting Interpreter, T1068: Exploitation for Privilege Escalation	https://live.paloaltonetworks.com/t5/expedition-release-notes/expedition-1-2-96-hotfix-information/ta-p/599340

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2021-26086	☒	Atlassian Jira Server and Data Center before version 8.5.14, from version 8.6.0 before 8.13.6, and from version 8.14.0 before 8.16.1	-
	ZERO-DAY		
	☒	**AFFECTED CPE**	**ASSOCIATED ATTACKS/RANSOMWARE**
NAME	**BAS ATTACKS**	cpe:2.3:a:atlassian:jira_data_center:*:*:*:*:*:*:*:*	Androxgh0st Botnet
Atlassian Jira Server and Data Center Path Traversal Vulnerability	☒		
	CWE ID	**ASSOCIATED TTPs**	**PATCH LINK**
	CWE-22	T1059: Command and Scripting Interpreter, T1068: Exploitation for Privilege Escalation	https://jira.atlassian.com/browse/JRASERVER-72695

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2014-2120	❌	Cisco Adaptive Security Appliance (ASA) Software WebVPN login page	-
	ZERO-DAY		
	❌	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS	cpe:2.3:o:cisco:adaptive_security_appliance_software:-:*:*:*:*:*:*:*	Androxgh0st Botnet
Cisco Adaptive Security Appliance (ASA) Cross-Site Scripting (XSS) Vulnerability	❌		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-79	T1059 : Command and Scripting Interpreter, T1189 : Drive-by Compromise	-

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2021-41277	✗	Metabase GeoJSON API	-
	ZERO-DAY		
	✗	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS	cpe:2.3:a:metabase:metabase:-:*:*:_:*:*:*	Androxgh0st Botnet
Metabase GeoJSON API Local File Inclusion Vulnerability	✓		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-200	T1059: Command and Scripting Interpreter, T1068: Exploitation for Privilege Escalation	https://github.com/metabase/metabase/commit/042a36e49574c749f944e19cf80360fd3dc322f0

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2024-43451	✗	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:*:*:*:*:*:*:*:*:*	-
NTLM Hash Disclosure Spoofing Vulnerability	✓		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-73	T1204: User Execution	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-43451

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2024-49039	✗	Windows: 10 - 11 24H2 Windows Server: 2016 - 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 Task Scheduler Elevation of Privilege Vulnerability	✗		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-287	T1068: Exploitation for Privilege Escalation	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-49039

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2019-16278	✗	Nostromo nhttpd	-
	ZERO-DAY		
	✗	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS	cpe:2.3:a:nazgul:nostromo_nhttpd:*:*:*:*:*:*:*:*	-
Nostromo nhttpd Directory Traversal Vulnerability	✓		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-22	T1068: Exploitation for Privilege Escalation	https://www.nazgul.ch/dev/nostromo_cl.txt

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2024-51567	✗	CyberPanel versions through 2.3.6 and (unpatched) 2.3.7	-
	ZERO-DAY		
	✓	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS	cpe:2.3:a:cyberpanel:cyberpanel:*:*:*:*:*:*:*:*	PSAUX Ransomware
CyberPanel Incorrect Default Permissions Vulnerability	✓		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-276	T1059: Command and Scripting Interpreter, T1068: Exploitation for Privilege Escalation	https://github.com/usmannasir/cyberpanel/commit/5b08cd6d53f4dbc2107ad9f555122ce8b0996515

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2024-43093	✗	Google Android	-
	ZERO-DAY		
	✗	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS	cpe:2.3:o:google:android:12.0:*:*:*:*:*:*:*	-
Android Framework Privilege Escalation Vulnerability	✗		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	-	T1059: Command and Scripting Interpreter, T1068: Exploitation for Privilege Escalation	https://android.googlesource.com/platform/frameworks/base/+/67d6e08322019f7ed8e3f80bd6cd16f8bcb809ed

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2024-5910	✗	Palo Alto Networks’ Expedition versions prior to 1.2.92	-
	ZERO-DAY		
	✗	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS	cpe:2.3:a:paloaltonetworks:expedition:*:*:*:*:*:*:*:*	-
Palo Alto Expedition Missing Authentication Vulnerability	✓		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-306	T1059: Command and Scripting Interpreter, T1078 : Valid Accounts, T1068 : Exploitation for Privilege Escalation	https://live.paloaltonetworks.com/t5/expedition-release-notes/expedition-1-2-96-hotfix-information/ta-p/599340

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2024-8956	✗	PTZOptics PT30X-SDI/NDI-xx before firmware 6.3.40	-
	ZERO-DAY		
	✗	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS	cpe:2.3:o:ptzoptics:pt30x-sdi_firmware:*:*:*:*:*:*:*:*	-
PTZOptics PT30X-SDI/NDI Cameras Authentication Bypass Vulnerability	✗		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-306	T1059: Command and Scripting Interpreter, T1078 : Valid Accounts, T1068 : Exploitation for Privilege Escalation	https://ptzoptics.com/latest-firmware-files/

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2024-8957	⊗	PTZOptics PT30X-SDI/NDI-xx before firmware 6.3.40	
	ZERO-DAY		
	⊗	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS	cpe:2.3:o:ptzoptics:pt30x-sdi_firmware:*:*:*:*:*:*:*:*	-
PTZOptics PT30X-SDI/NDI Cameras OS Command Injection Vulnerability	⊗		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-78	T1059: Command and Scripting Interpreter	https://ptzoptics.com/latest-firmware-files/

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.

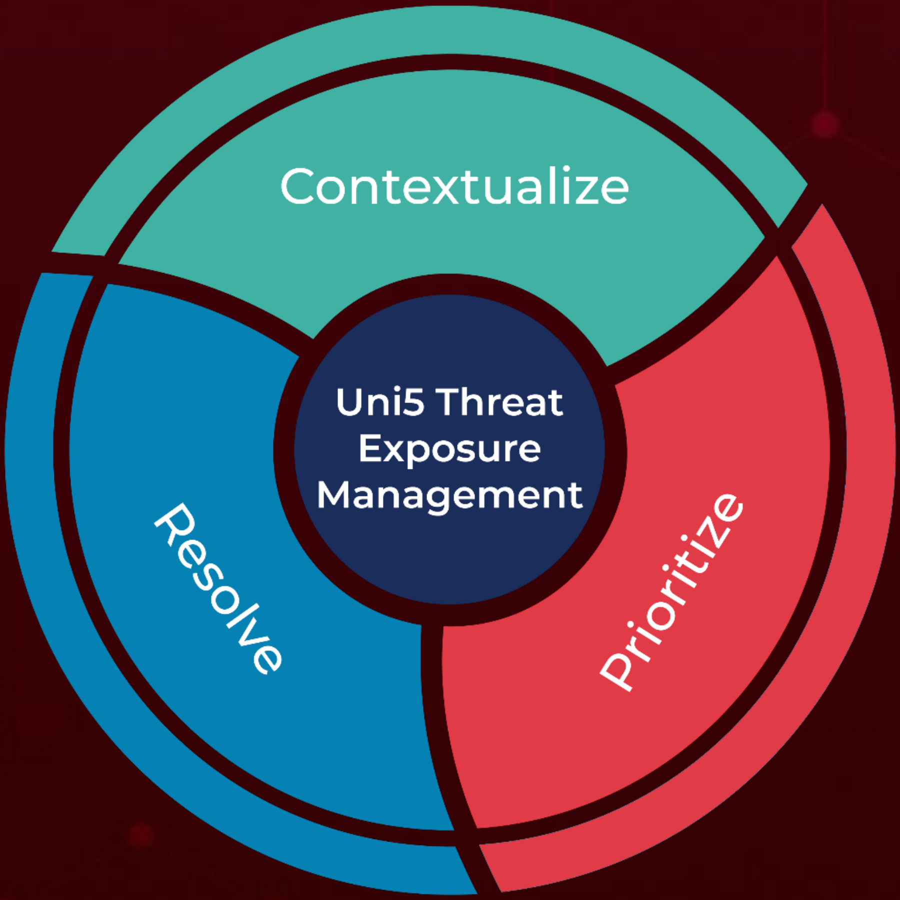
BAS Attacks: “BAS attacks” are the simulated cyber-attacks that can be carried out by our in-house Uni5's Breach and Attack Simulation (BAS), which organizations could use to identify vulnerabilities and improve their overall security posture.

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

December 3, 2024 • 9:00 PM

More at www.hivepro.com