

Date of Publication
January 6, 2025



HiveForce Labs

CISA

KNOWN

EXPLOITED

VULNERABILITY

CATALOG

December 2024

Table of Contents

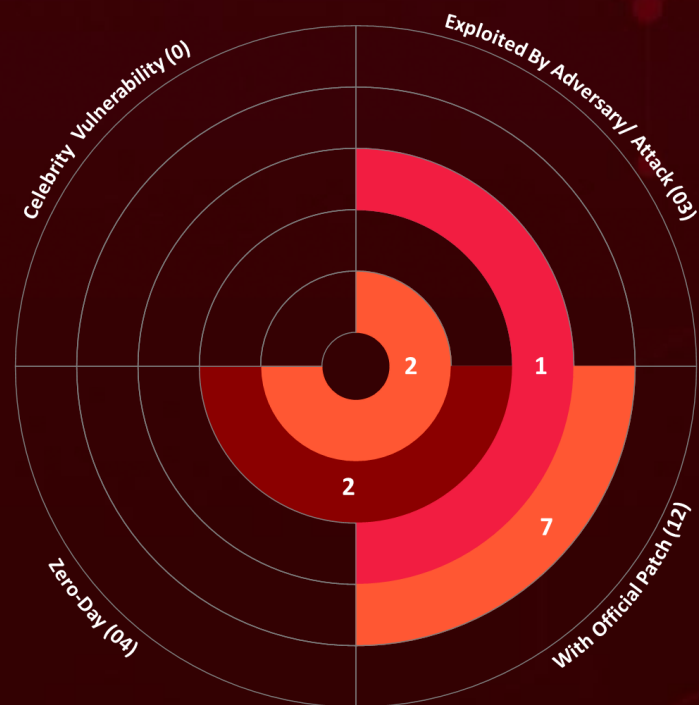
<u>Summary</u>	03
<u>CVEs List</u>	04
<u>CVEs Details</u>	06
<u>Recommendations</u>	16
<u>References</u>	17
<u>Appendix</u>	17
<u>What Next?</u>	18

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 December 2024, **sixteen** vulnerabilities met the criteria for inclusion in the CISA's KEV catalog. Of these, **four** are **zero-day** vulnerabilities; **three** have been **exploited** by known threat actors and employed in attacks.






16
Known Exploited
Vulnerabilities











CVEs List




CVE	NAME	AFFECTED PRODUCT	CVSS 3.x SCORE	ZERO-DAY	PATCH	DUE DATE
CVE-2024-3393	Palo Alto Networks PAN-OS Malformed DNS Packet Vulnerability	Palo Alto Networks PAN-OS	8.7			January 20, 2025
CVE-2021-44207	Acclaim Systems USAHERDS Use of Hard-Coded Credentials Vulnerability	Acclaim Systems USAHERDS	8.1			January 13, 2025
CVE-2024-12356	BeyondTrust Privileged Remote Access (PRA) and Remote Support (RS) Command Injection Vulnerability	BeyondTrust Privileged Remote Access (PRA) and Remote Support (RS)	9.8			December 27, 2024
CVE-2021-40407	Reolink RLC-410W IP Camera OS Command Injection Vulnerability	Reolink RLC-410W IP Camera	9.8			January 8, 2025
CVE-2019-11001	Reolink Multiple IP Cameras OS Command Injection Vulnerability	Reolink Multiple IP Cameras	7.2			January 8, 2025
CVE-2022-23227	NUUO NVRmini 2 Devices Missing Authentication Vulnerability	NUUO NVRmini2 Devices	9.8			January 8, 2025
CVE-2018-14933	NUUO NVRmini Devices OS Command Injection Vulnerability	NUUO NVRmini Devices	9.8			January 8, 2025
CVE-2024-55956	Cleo Multiple Products Unauthenticated File Upload Vulnerability	Cleo Multiple Products	9.8			January 7, 2025
CVE-2024-35250	Microsoft Windows Kernel-Mode Driver Untrusted Pointer Dereference Vulnerability	Microsoft Windows	7.8			January 6, 2025




CVE	NAME	AFFECTED PRODUCT	CVSS 3.x SCORE	ZERO-DAY	PATCH	DUE DATE
CVE-2024-20767	Adobe ColdFusion Improper Access Control Vulnerability	Adobe ColdFusion	7.4			January 6, 2025
CVE-2024-50623	Cleo Multiple Products Unrestricted File Upload Vulnerability	Cleo Multiple Products	9.8			January 3, 2025
CVE-2024-49138	Microsoft Windows Common Log File System (CLFS) Driver Heap-Based Buffer Overflow Vulnerability	Microsoft Windows	7.8			December 31, 2024
CVE-2024-51378	CyberPanel Incorrect Default Permissions Vulnerability	CyberPersons CyberPanel	9.8			December 25, 2024
CVE-2024-11667	Zyxel Multiple Firewalls Path Traversal Vulnerability	Zyxel Multiple Firewalls	9.8			December 24, 2024
CVE-2024-11680	ProjectSend Improper Authentication Vulnerability	ProjectSend	9.8			December 24, 2024
CVE-2023-45727	North Grid Proself Improper Restriction of XML External Entity (XXE) Reference Vulnerability	North Grid Proself	7.5			December 24, 2024





CVEs Details





CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2024-3393		PAN-OS 11.2: Versions below 11.2.3; PAN-OS 11.1: Versions below 11.1.5; PAN-OS 10.2: Versions upto 10.2.8, Versions below 10.2.10- h12 and Versions below 10.2.13-h2; PAN-OS 10.1: Versions upto 10.1.14 and Versions below 10.1.14-h8	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS	cpe:2.3:o:paloaltonetworks:pan-os:*.~*~*~*~*~*~*	-
Palo Alto Networks PAN-OS Malformed DNS Packet Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-754	T1498: Network Denial of Service, T1068: Exploitation for Privilege Escalation	https://security.paloaltonetworks.com/CVE-2024-3393





CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2021-44207		Acclaim USAHERDS through 7.4.0.1	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS	cpe:2.3:a:acclaimsystems:usaherds:*:*:*:*:*:*	-
Acclaim Systems USAHERDS Use of Hard-Coded Credentials Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-798	T1078: Valid Accounts, T1210: Exploitation of Remote Services	https://github.com/mandiant/Vulnerability-Disclosures/blob/master/MNDT-2021-0012/MNDT-2021-0012.md


CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2024-12356		BeyondTrust Privileged Remote Access (PRA) version 24.3.1 and earlier, Remote Support (RS) version 24.3.1 and earlier	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS	cpe:2.3:a:beyondtrust:privileged_remote_access:*:*:*:*:*:* cpe:2.3:a:beyondtrust:remote_support:*:*:*:*:*:*	-
BeyondTrust Privileged Remote Access (PRA) and Remote Support (RS) Command Injection Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-77	T1068: Exploitation for Privilege Escalation, T1059: Command and Scripting Interpreter	https://www.beyondtrust.com/trust-center/security-advisories/bt24-10




CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2021-40407		Reolink RLC-410W v3.0.0.136_20121102	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS	cpe:2.3:o:reolink:rlc-410w_firmware:3.0.0.136_20121102:*:*:*:*:*:*	-
Reolink RLC-410W IP Camera OS Command Injection Vulnerability		cpe:2.3:h:reolink:rlc-410w:-:*:*:*:*:*:*	-
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-78	T1059: Command and Scripting Interpreter	EOL




CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2019-11001		Reolink RLC-410W, C1 Pro, C2 Pro, RLC-422W, and RLC-511W devices through 1.0.227	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS	cpe:2.3:o:reolink:c1_pro_firmware:*:*:*:*:*:*	-
Reolink Multiple IP Cameras OS Command Injection Vulnerability		cpe:2.3:h:reolink:c1_pro:-:*:*:*:*:*:*	-
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-78	T1059: Command and Scripting Interpreter	




CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2022-23227		NUUO NVRmini2 through 3.11	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS	cpe:2.3:o:nuuo:nvrmini2_firmware:*:*:*:*:*:*	-
NUUO NVRmini 2 Devices Missing Authentication Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-306	T1556: Modify Authentication Process, T1078: Valid Accounts	




CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2018-14933		NUUO NVRmini Devices	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS	cpe:2.3:o:nuuo:nvrmini_firmware:2016:*:*:*:*:*:*	-
NUUO NVRmini Devices OS Command Injection Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-78	T1059: Command and Scripting Interpreter	




CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2024-55956		Cleo Harmony (versions upto 5.8.0.21), Cleo VLTrader (versions upto 5.8.0.21), Cleo LexiCom (versions upto 5.8.0.21)	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS	cpe:2.3:a:cleo:vltrader:*:*:*:*:*:* *:*:*:*	ClOp Ransomware
Cleo Multiple Products Unauthenticated File Upload Vulnerability		cpe:2.3:a:cleo:lexicom:*:*:*:*:*:* *:*:*:* cpe:2.3:a:cleo:harmony:*:*:*:*:*:* *:*:*:*	
	CWE ID	ASSOCIATED TTPs	
	CWE-77 CWE-276	T1059: Command and Scripting Interpreter, T1105: Ingress Tool Transfer	https://support.cleo.com/hc/en-us/articles/28408134019735-Cleo-Product-Security-Update-CVE-2024-55956




CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR		
CVE-2024-35250		Windows: 10 - 11 23H2 Windows Server: 2008 - 2022 23H2	-		
	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 Kernel-Mode Driver Untrusted Pointer Dereference Vulnerability		CWE ID		ASSOCIATED TTPs	PATCH LINK
	CWE-119 CWE-822	T1068: Exploitation for Privilege Escalation, T1078: Valid Accounts		https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-35250	




CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2024-20767		Adobe ColdFusion versions 2023.6, 2021.12 and earlier	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS	cpe:2.3:a:adobe:coldfusion:2021:-:*:*:*:*:*	-
Adobe ColdFusion Improper Access Control Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-284	T1190: Exploit Public-Facing Application, T1203: Exploitation for Client Execution	https://helpx.adobe.com/security/products/coldfusion/apsb24-14.html

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2024-50623		Cleo Harmony (versions upto 5.8.0.21), Cleo VLTrader (versions upto 5.8.0.21), Cleo LexiCom (versions upto 5.8.0.21)	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS	cpe:2.3:a:cleo:vltrader:*:*:*:*:*:*:*	ClOp Ransomware
Cleo Multiple Products Unrestricted File Upload Vulnerability		cpe:2.3:a:cleo:lexicom:*:*:*:*:*:*:*	
		cpe:2.3:a:cleo:harmony:*:*:*:*:*:*:*	
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-434	T1059: Command and Scripting Interpreter, T1105: Ingress Tool Transfer	https://support.cleo.com/hc/en-us/articles/27140294267799-Cleo-Product-Security-Advisory-CVE-2024-50623

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2024-49138		Windows: 10 - 11 24H2 Windows Server: 2008 - 2025	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS	cpe:2.3:o:microsoft:windows:*:*:*:*:*:*	
Microsoft Windows Common Log File System (CLFS) Driver Heap-Based Buffer Overflow Vulnerability		cpe:2.3:o:microsoft:windows_server:*:*:*:*:*:*	-
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-122	T1068: Exploitation for Privilege Escalation	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-49138

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2024-51378		Cyber Panel before 1c0c6cb	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS	cpe:2.3:a:cyberpanel:cyberpanel:*:*:*:*:*:*	
CyberPanel Incorrect Default Permissions Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-78 CWE-276	T1190: Exploit Public-Facing Application, T1203: Exploitation for Client Execution	https://github.com/umannasir/cyberpanel/commit/1c0c6cbcf71abe573da0b5fddfb9603e7477f683

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2024-11667		Zyxel ATP series Version 5.00 - 5.38, Zyxel USG FLEX series Version 5.00 - 5.38, Zyxel USG FLEX 50W Version 5.10 - 5.38, Zyxel USG20W-VPN Version 5.10 - 5.38	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS	cpe:2.3:o:zyxel:atp_firmware:*:*:*:*:*:*	
Zyxel Multiple Firewalls Path Traversal Vulnerability		cpe:2.3:o:zyxel:usg_flex_firmware:*:*:*:*:*:* cpe:2.3:o:zyxel:usg_flex_50w_firmware:*:*:*:*:*:* cpe:2.3:o:zyxel:usg20-vpn_firmware:*:*:*:*:*:*	Helldown Ransomware
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-22	T1059: Command and Scripting, T1136 : Create Account	https://www.zyxel.com/us/en-us/support/download

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2024-11680		ProjectSend versions prior to r1720	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS	cpe:2.3:a:projectsend:projectsend:*:*:*:*:*:*	-
ProjectSend Improper Authentication Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-863 CWE-287	T1078: Valid Accounts	https://github.com/projectsend/projectsend/commit/193367d937b1a59ed5b68dd4e60bd53317473744

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2023-45727		North Grid Proself Enterprise/Standard Edition Ver5.62 and earlier, Proself Gateway Edition Ver1.65 and earlier, Proself Mail Sanitize Edition Ver1.08	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS	cpe:2.3:a:northgrid:proself:*:*:*:*:mail_sanitize:*:*:* cpe:2.3:a:northgrid:proself:*:*:*:*:gateway:*:*:* cpe:2.3:a:northgrid:proself:*:*:*:*:enterprise:*:*:* cpe:2.3:a:northgrid:proself:*:*:*:*:standard:*:*:*	-
North Grid Proself Improper Restriction of XML External Entity (XXE) Reference Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-611	T1059: Command and Scripting Interpreter, T1005: Data from Local System, T1046: Network Service Discovery	https://www.proself.jp/information/153/

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.

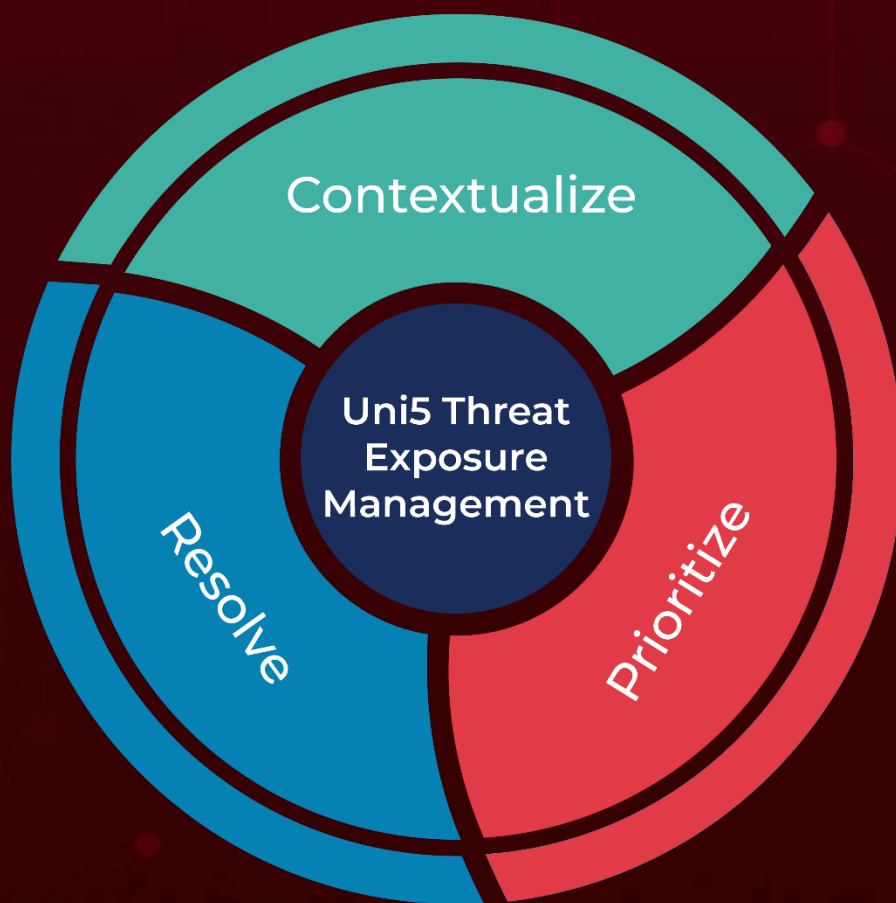
BAS Attacks: “BAS attacks” are the simulated cyber-attacks that can be carried out by our in-house Uni5's Breach and Attack Simulation (BAS), which organizations could use to identify vulnerabilities and improve their overall security posture.

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

January 6, 2025 • 5:30 AM

© 2025 All Rights are Reserved by Hive Pro



More at www.hivepro.com