Date of Publication
May 6, 2024

Hive Pro

Hiveforce Labs

CISA KNOWN EXPLOITED VULNERABILITY CATALOG

April 2024

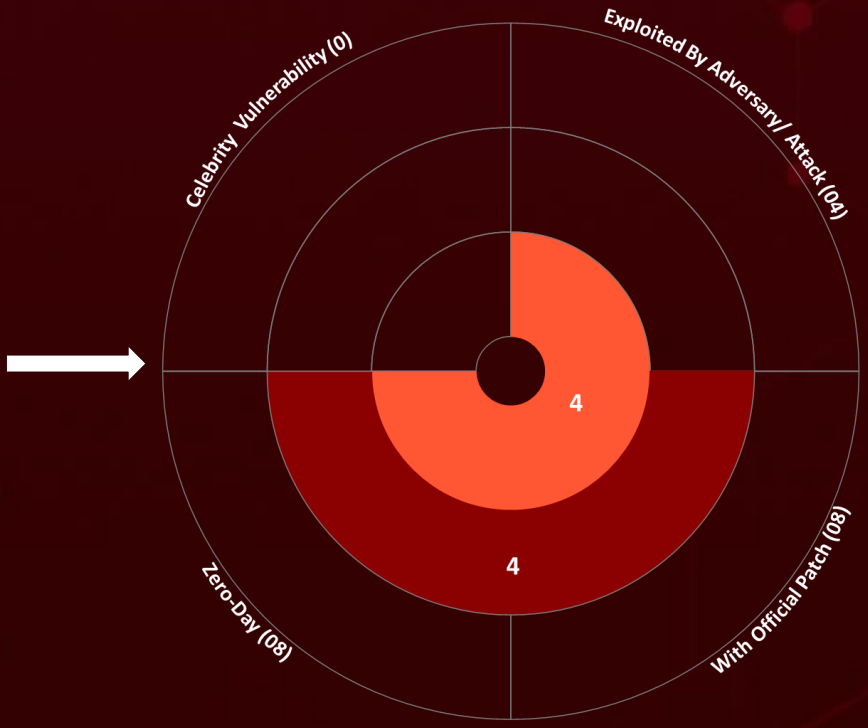
Table of Contents

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

10
Known Exploited Vulnerabilities



CVEs List

CVE	NAME	AFFECTED PRODUCT	CVSS 3.x SCORE	ZERO-DAY	PATCH	DUE DATE
CVE-2024-29748	Google Pixel Privilege Escalation Vulnerability	Google Pixel	7.8	✓	✓	April 25, 2024
CVE-2024-29745	Google Pixel Information Disclosure Vulnerability	Google Pixel	5.5	✓	✓	April 25, 2024
CVE-2024-3273	D-Link Multiple NAS Devices Command Injection Vulnerability	D-Link Multiple NAS Devices	7.3	✗	✗	May 2, 2024
CVE-2024-3272	D-Link Multiple NAS Devices Use of Hard-Coded Credentials Vulnerability	D-Link Multiple NAS Devices	9.8	✗	✗	May 2, 2024
CVE-2024-3400	Palo Alto Networks PAN-OS Command Injection Vulnerability	Palo Alto Networks PAN-OS	10	✓	✓	April 19, 2024
CVE-2022-38028	Microsoft Windows Print Spooler Privilege Escalation Vulnerability	Microsoft Windows	7.8	✓	✓	May 14, 2024
CVE-2024-4040	CrushFTP VFS Sandbox Escape Vulnerability	CrushFTP	10	✓	✓	May 1, 2024
CVE-2024-20359	Cisco ASA and FTD Privilege Escalation Vulnerability	Cisco Adaptive Security Appliance (ASA) and Firepower Threat Defense (FTD)	6	✓	✓	May 1, 2024
CVE-2024-20353	Cisco ASA and FTD Denial of Service Vulnerability	Cisco Adaptive Security Appliance (ASA) and Firepower Threat Defense (FTD)	8.6	✓	✓	May 1, 2024
CVE-2024-29988	Microsoft SmartScreen Prompt Security Feature Bypass Vulnerability	Microsoft SmartScreen Prompt	8.8	✓	✓	May 21, 2024

CVEs Details

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2024-29748	✗ ZERO-DAY	Google Pixel	-
	✓	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS	cpe:2.3:o:google:android:-:*:*:*:*:*:*:* cpe:2.3:h:google:pixel:-:*:*:*:*:*:*:*	-
Google Pixel Privilege Escalation Vulnerability	✗		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-20	T1068 : Exploitation for Privilege Escalation	https://source.android.com/docs/security/bulletin/pixel/2024-04-01

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2024-29745	✗ ZERO-DAY	Google Pixel	-
	✓	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS	cpe:2.3:o:google:android:-:*:*:*:*:*:*:*	-
Google Pixel Information Disclosure Vulnerability	✗		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-908	T1426: System Information Discovery	https://source.android.com/docs/security/bulletin/pixel/2024-04-01

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2024-3273	✗	DNS-320L Version 1.11, Version 1.03.0904.2013, Version 1.01.0702.2013 DNS-325 Version 1.01 DNS-327L Version 1.09, Version 1.00.0409.2013 DNS-340L Version 1.08	-
	ZERO-DAY		
	✗	**AFFECTED CPE**	**ASSOCIATED ATTACKS/RANSOMWARE**
NAME	**BAS ATTACKS**	cpe:2.3:a:d-link:dns-320l:*:*:*:*:*:*:*:* cpe:2.3:a:d-link:dns-325:*:*:*:*:*:*:*:* cpe:2.3:a:d-link:dns-327l:*:*:*:*:*:*:*:* cpe:2.3:a:d-link:dns-340l:*:*:*:*:*:*:*:*	-
D-Link Multiple NAS Devices Command Injection Vulnerability	✓		
	CWE ID	**ASSOCIATED TTPs**	**MITIGATION DETAILS**
	CWE-77	T1059: Command and Scripting Interpreter	The affected D-Link NAS devices are no longer supported. Users are advised to retire them and replace them with newer, supported NAS devices.

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2024-3272	✗	D-Link DNS-320L, D-Link DNS-325, D-Link DNS-327L, D-Link DNS-340L: All versions	-
	ZERO-DAY		
	✗	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS	cpe:2.3:h:dlink:dns-320l:-:*:*:*:*:*:*:* cpe:2.3:h:dlink:dns-325:-:*:*:*:*:*:*:* cpe:2.3:h:dlink:dns-327l:-:*:*:*:*:*:*:* cpe:2.3:h:dlink:dns-340l:-:*:*:*:*:*:*:*	-
D-Link Multiple NAS Devices Use of Hard-Coded Credentials Vulnerability	✓		
	CWE ID	ASSOCIATED TTPs	MITIGATION DETAILS
	CWE-798	T1552: Unsecured Credentials	The affected D-Link NAS devices are no longer supported. Users are advised to retire them and replace them with newer, supported NAS devices.

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2024-3400	✗	Palo Alto PAN-OS: 10.2 < 10.2.9-h1 Palo Alto PAN-OS: 11.0 <11.0.4-h1 Palo Alto PAN-OS: 11.1 < 11.1.2-h3 11.1.2-h2	UTA0218
	ZERO-DAY		
	✓	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS	cpe:2.3:a:paloaltonetworks:pan-os:*:*:*:*:*:*:*:*	UPSTYLE
Palo Alto Networks PAN-OS Command Injection Vulnerability	✓		
	CWE ID	ASSOCIATED TTPs	PATCH LINKS
	CWE-77	T1059: Command and Scripting Interpreter	https://security.paloaltonetworks.com/CVE-2024-3400

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2022-38028	✗ ZERO-DAY	Microsoft Windows Print Spooler	APT28
	✓	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS	cpe:2.3:o:microsoft:windows:*:*:*:*:*:*:*:*	GooseEgg
Microsoft Windows Print Spooler Privilege Escalation Vulnerability	✓		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-264	T1068: Exploitation for Privilege Escalation	https://msrc.microsoft.com/update-guide/en-US/advisory/CVE-2022-38028

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2024-4040	✗ ZERO-DAY	CrushFTP versions prior to 10.7.1 and 11.1.0	-
	✓	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS	cpe:2.3:a:crushftp:crushftp:*:*:*:*:*:*:*:*	-
CrushFTP VFS Sandbox Escape Vulnerability	✗		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-1336	T1059: Command and Scripting Interpreter	https://www.crushftp.com/download.html

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2024-20359	✗ ZERO-DAY	Cisco ASA Software or FTD Software	STORM-1849
	✓	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS	cpe:2.3:o:cisco:adaptive_security_appliance_software:*:*:*:*:*:*:*:*	-
Cisco ASA and FTD Privilege Escalation Vulnerability	✗		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-94	T1068: Exploitation for Privilege Escalation	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-persist-rce-FLsNXF4h

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2024-20353	✗ ZERO-DAY	Cisco ASA Software and FTD Software	STORM-1849
	✓	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS	cpe:2.3:o:cisco:adaptive_security_appliance_software:*:*:*:*:*:*:*:*	-
Cisco ASA and FTD Denial of Service Vulnerability	✗		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-835	T1498: Network Denial of Service	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-websrvs-dos-X8gNucD2

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2024-29988	✗	Windows: 10 - 11 23H2 Windows Server: 2019 - 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 SmartScreen Prompt Security Feature Bypass Vulnerability	✗		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-693	T1190: Exploit Public-Facing Application, T1040: Network Sniffing	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-29988

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.

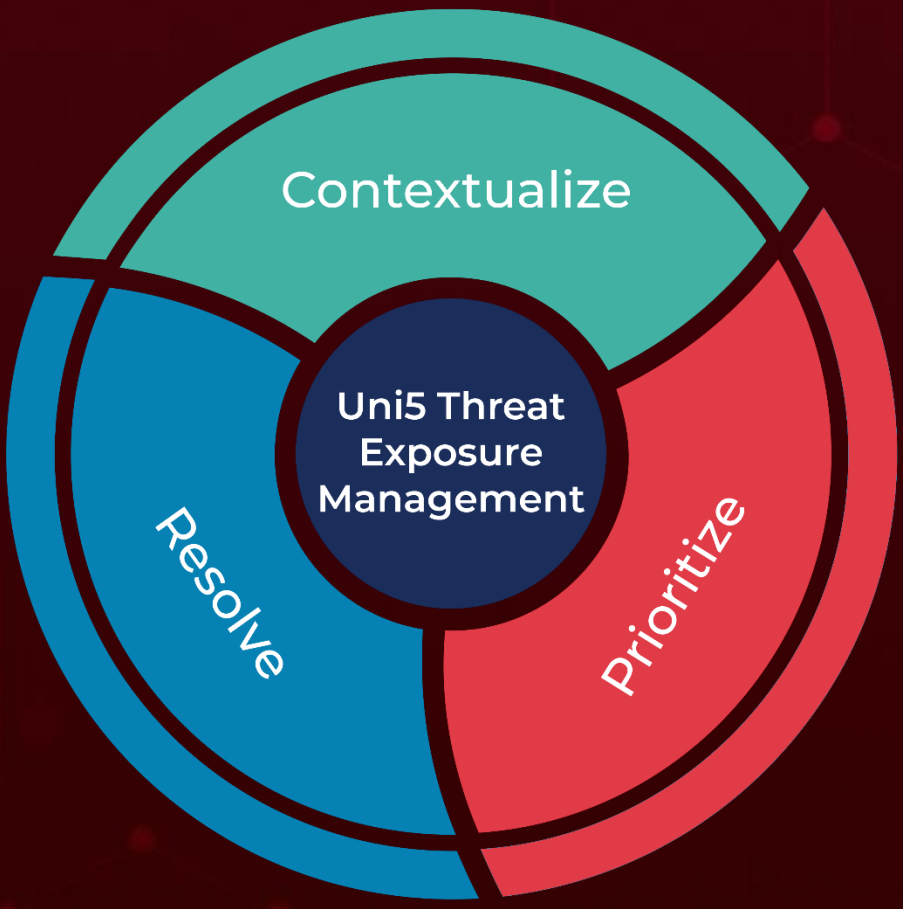
BAS Attacks: “BAS attacks” are the simulated cyber-attacks that can be carried out by our in-house Uni5's Breach and Attack Simulation (BAS), which organizations could use to identify vulnerabilities and improve their overall security posture.

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

May 6, 2024 . 1:30 AM

More at www.hivepro.com