Date of Publication
October 1, 2024

Hive Pro

HiveForce Labs

CISA KNOWN EXPLOITED VULNERABILITY CATALOG

September 2024

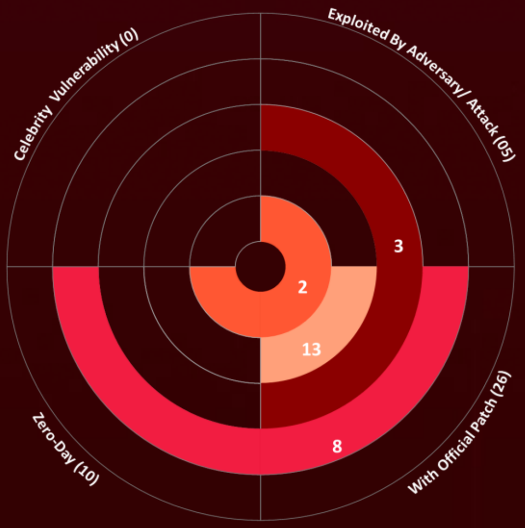
Table of Contents

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

26
Known Exploited Vulnerabilities



CVEs List

CVE	NAME	AFFECTED PRODUCT	CVSS 3.x SCORE	ZERO-DAY	PATCH	DUE DATE
CVE-2024-7262	Kingsoft WPS Office Path Traversal Vulnerability	Kingsoft WPS Office	7.8	✓	✓	September 24, 2024
CVE-2021-20124	Draytek VigorConnect Path Traversal Vulnerability	Draytek VigorConnect	7.5	✗	✓	September 24, 2024
CVE-2021-20123	Draytek VigorConnect Path Traversal Vulnerability	Draytek VigorConnect	7.5	✗	✓	September 24, 2024
CVE-2024-40766	SonicWall SonicOS Improper Access Control Vulnerability	SonicWall SonicOS	9.8	✗	✓	September 30, 2024
CVE-2017-1000253	Linux Kernel PIE Stack Buffer Corruption Vulnerability	Linux Kernel	7.8	✗	✓	September 30, 2024
CVE-2016-3714	ImageMagick Improper Input Validation Vulnerability	ImageMagick	8.4	✓	✓	September 30, 2024
CVE-2024-38217	Microsoft Windows Mark of the Web (MOTW) Protection Mechanism Failure Vulnerability	Microsoft Windows	5.4	✓	✓	October 1, 2024
CVE-2024-38014	Microsoft Windows Installer Improper Privilege Management Vulnerability	Microsoft Windows	7.8	✓	✓	October 1, 2024
CVE-2024-38226	Microsoft Publisher Protection Mechanism Failure Vulnerability	Microsoft Publisher	7.3	✓	✓	October 1, 2024
CVE-2024-8190	Ivanti Cloud Services Appliance OS Command Injection Vulnerability	Ivanti Cloud Services Appliance	7.2	✗	✓	October 4, 2024

CVE	NAME	AFFECTED PRODUCT	CVSS 3.x SCORE	ZERO-DAY	PATCH	DUE DATE
CVE-2024-6670	Progress WhatsUp Gold SQL Injection Vulnerability	Progress WhatsUp Gold	9.8	✗	✓	October 7, 2024
CVE-2024-43461	Microsoft Windows MSHTML Platform Spoofing Vulnerability	Microsoft Windows	8.8	✓	✓	October 7, 2024
CVE-2014-0502	Adobe Flash Player Double Free Vulnerablity	Adobe Flash Player	8.8	✓	✓	October 8, 2024
CVE-2013-0648	Adobe Flash Player Code Execution Vulnerability	Adobe Flash Player	8.8	✓	✓	October 8, 2024
CVE-2013-0643	Adobe Flash Player Incorrect Default Permissions Vulnerability	Adobe Flash Player	8.8	✓	✓	October 8, 2024
CVE-2014-0497	Adobe Flash Player Integer Underflow Vulnerablity	Adobe Flash Player	9.8	✓	✓	October 8, 2024
CVE-2020-14644	Oracle WebLogic Server Remote Code Execution Vulnerability	Oracle WebLogic Server	9.8	✗	✓	October 9, 2024
CVE-2022-21445	Oracle ADF Faces Deserialization of Untrusted Data Vulnerability	Oracle ADF Faces	9.8	✗	✓	October 9, 2024
CVE-2020-0618	Microsoft SQL Server Reporting Services Remote Code Execution Vulnerability	Microsoft SQL Server	8.8	✗	✓	October 9, 2024
CVE-2024-27348	Apache HugeGraph-Server Improper Access Control Vulnerability	Apache HugeGraph-Server	9.8	✗	✓	October 9, 2024
CVE-2024-8963	Ivanti Cloud Services Appliance (CSA) Path Traversal Vulnerability	Ivanti Cloud Services Appliance (CSA)	9.1	✗	✓	October 10, 2024
CVE-2024-7593	Ivanti Virtual Traffic Manager Authentication Bypass Vulnerability	Ivanti Virtual Traffic Manager	9.8	✗	✓	October 15, 2024

CVE	NAME	AFFECTED PRODUCT	CVSS 3.x SCORE	ZERO-DAY	PATCH	DUE DATE
CVE-2019-0344	SAP Commerce Cloud Deserialization of Untrusted Data Vulnerability	SAP Commerce Cloud	9.8	✗	✓	October 21, 2024
CVE-2021-4043	Motion Spell GPAC Null Pointer Dereference Vulnerability	Motion Spell GPAC	5.5	✗	✓	October 21, 2024
CVE-2020-15415	DrayTek Multiple Vigor Routers OS Command Injection Vulnerability	DrayTek Multiple Vigor Routers	9.8	✗	✓	October 21, 2024
CVE-2023-25280	D-Link DIR-820 Router OS Command Injection Vulnerability	D-Link DIR-820 Router	9.8	✗	✓	October 21, 2024

CVEs Details

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2024-7262	✗	Kingsoft WPS Office version from 12.2.0.13110 to 12.1.0.16412	APT-C-60 (aka False Hunter, Pseudo Hunter)
	ZERO-DAY		
	✓	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS	cpe:2.3:a:kingsoft:wps_office:*:*:*:*:*:*:*:*	SpyGlace Backdoor
Kingsoft WPS Office Path Traversal Vulnerability	✓		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-22	T1203: Exploitation for Client Execution T1204.002: Malicious File	https://www.wps.com/download/

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2021-20124	⊗	Draytek VigorConnect 1.6.0-B3	-
	ZERO-DAY		
	⊗	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS	cpe:2.3:a:draytek:vigorconnect:1.6.0:beta3:*:*:*:*:*:*	-
Draytek VigorConnect Path Traversal Vulnerability	⊗		
	CWE ID	ASSOCIATED TTPs	PATCH LINKS
	CWE-22	T1068: Exploitation for Privilege Escalation; T1020: Automated Exfiltration	Upgrade to VigorConnect 1.6.1

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2021-20123	⊗	Draytek VigorConnect 1.6.0-B3	-
	ZERO-DAY		
	⊗	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS	cpe:2.3:a:draytek:vigorconnect:1.6.0:beta3:*:*:*:*:*:*	-
Draytek VigorConnect Path Traversal Vulnerability	⊗		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-22	T1068: Exploitation for Privilege Escalation; T1020: Automated Exfiltration	Upgrade to VigorConnect 1.6.1

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2024-40766	⊗	SonicWall SonicOS SOHO (Gen 5) version 5.9.2.14-12o and older, Gen6 Firewalls Version 6.5.4.14-109n and older, Gen7 Firewalls SonicOS build version 7.0.1-5035 and older	Akira ransomware group
	ZERO-DAY		
	⊗	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS	cpe:2.3:a:sonicwall:sonicos:*:*:*:*:*:*:*:*	-
SonicWall SonicOS Improper Access Control Vulnerability	⊗		
	CWE ID	ASSOCIATED TTPs	PATCH LINKS
	CWE-284	T1068: Exploitation for Privilege Escalation; T1078: Valid Accounts	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2024-0015

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2017-1000253	⊗	Centos Version: 6.0-6.9, 7.1406, 7.1503, 7.1511, 7.1611, redhat, linux	-
	ZERO-DAY		
	⊗	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS	cpe:2.3:o:centos:centos:*:*:*:*:*:*:*:* cpe:2.3:o:redhat:enterprise_linux:*:*:*:*:*:*:*:* cpe:2.3:o:linux:linux_kernel:*:*:*:*:*:*:*:*:*	-
Linux Kernel PIE Stack Buffer Corruption Vulnerability	⊗		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-119	T1068: Exploitation for Privilege Escalation; T1059: Command and Scripting Interpreter	https://git.kernel.org/pub/scm/linux/kernel/git/torvalds/linux.git/commit/?id=a87938b2e246b81b4fb713edb371a9fa3c5c3c86 , https://access.redhat.com/security/cve/CVE-2017-1000253

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2016-3714	✗	EPHEMERAL, HTTPS, MVG, MSL, TEXT, WIN, and PLT coders in ImageMagick before 6.9.3-10 and 7.x before 7.0.1-1	-
	ZERO-DAY		
	✓	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS	cpe:2.3:a:imagemagick:imagemagick:*:*:*:*:*:*:*:*	-
ImageMagick Improper Input Validation Vulnerability	✗		
	CWE ID	ASSOCIATED TTPs	PATCH LINKS
	CWE-20	T1059: Command and Scripting Interpreter; T1036.008: Masquerade File Type	Upgrade to ImageMagick version 6.9.3-10 and 7.0.1-1

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2024-38217	✗	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 Mark of the Web (MOTW) Protection Mechanism Failure Vulnerability	✗		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-693	T1553.005: Mark-of-the-Web Bypass, T1204: User Execution	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38217

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2024-38014	✗	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:*:*:*:*:*:*:*:*	-
Microsoft Windows Installer Improper Privilege Management Vulnerability	✗		
	CWE ID	ASSOCIATED TTPs	PATCH LINKS
	CWE-269	T1068: Exploitation for Privilege Escalation	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38014

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2024-38226	✗	Microsoft Publisher 2016 Microsoft Office LTSC 2021 Microsoft Office 2019	-
	ZERO-DAY		
	✓	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS	cpe:2.3:a:microsoft:publisher:*:*:*:*:*:*:*:*	-
Microsoft Publisher Protection Mechanism Failure Vulnerability	✗		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-693	T1553: Subvert Trust Controls, T1204: User Execution	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38226

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2024-8190	⊗	CSA 4.6 (All versions before Patch 519)	-
	ZERO-DAY		
	⊗	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS	cpe:2.3:a:ivanti:endpoint_manager_cloud_services_appliance:4.6:-:*:*:*:*:*:* cpe:2.3:a:ivanti:endpoint_manager_cloud_services_appliance:4.6:patch_512:*:*:*:*:*:*	-
Ivanti Cloud Services Appliance OS Command Injection Vulnerability	⊗		
	CWE ID	ASSOCIATED TTPs	PATCH LINKS
	CWE- 78	T1059: Command and Scripting Interpreter T1190: Exploit Public-Facing Application	https://forums.ivanti.com/s/article/CSA-4-6-Patch-519 , https://forums.ivanti.com/s/article/CSA-5-0-Download

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2024-6670	⊗	Progress WhatsUp Gold versions released before 2024.0.0	-
	ZERO-DAY		
	⊗	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS	cpe:2.3:a:progress:whatsup_gold:*:*:*:*:*:*:*:*	-
Progress WhatsUp Gold SQL Injection Vulnerability	⊗		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-89	T1059: Command and Scripting Interpreter	https://community.progress.com/s/article/WhatsUp-Gold-Security-Bulletin-August-2024

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2024-43461	✗	Windows: 10 - 11 23H2 Windows Server: 2008 - 2022 23H2	Void Banshee APT
	ZERO-DAY		
	✓	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS	cpe:2.3:o:microsoft:windows:*:*:*:*:*:*:*:* cpe:2.3:o:microsoft:windows_server:*:*:*:*:*:*:*:*	Atlantida
Microsoft Windows MSHTML Platform Spoofing Vulnerability	✗		
	CWE ID	ASSOCIATED TTPs	PATCH LINKS
	CWE-451	T1059: Command and Scripting Interpreter, T1204: User Execution	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-43461

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2014-0502	✗	Adobe Flash Player before 11.7.700.269 and 11.8.x through 12.0.x before 12.0.0.70 on Windows and Mac OS X and before 11.2.202.341 on Linux, Adobe AIR before 4.0.0.1628 on Android, Adobe AIR SDK before 4.0.0.1628, and Adobe AIR SDK & Compiler before 4.0.0.1628	-
	ZERO-DAY		
	✓	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS	cpe:2.3:a:adobe:flash_player:*:*:*:*:*:*:*:* cpe:2.3:o:apple:mac_os_x:-:*:*:*:*:*:*:* cpe:2.3:o:microsoft:windows:-:*:*:*:*:*:*:* cpe:2.3:a:adobe:adobe_air_sdk:*:*:*:*:*:*:*:* cpe:2.3:o:linux:linux_kernel:-:*:*:*:*:*:*:* cpe:2.3:a:adobe:adobe_air:*:*:*:*:*:*:*:* cpe:2.3:o:google:android:-:*:*:*:*:*:*:*	-
Adobe Flash Player Double Free Vulnerability	✗		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-415	T1059: Command and Scripting Interpreter	https://security.gentoo.org/glsa/201405-04 , https://lists.opensuse.org/archives/list/security-announce@lists.opensuse.org/message/T2FFA6C27X6ACZPQSGGSKSSQ5TALLIHZ/ , https://access.redhat.com/errata/RHSA-2014:0196.html , https://lists.opensuse.org/archives/list/security-announce@lists.opensuse.org/message/MQKCKOSL55LVRI4SWNRZUSOYFEORHU7I/

CVE ID	**CELEBRITY VULNERABILITY**	**AFFECTED PRODUCTS**	**ASSOCIATED ACTOR**
CVE-2013-0648	✗	Adobe Flash Player before 10.3.183.67 and 11.x before 11.6.602.171 on Windows and Mac OS X, and before 10.3.183.67 and 11.x before 11.2.202.273 on Linux	-
	ZERO-DAY		
	✓	**AFFECTED CPE**	**ASSOCIATED ATTACKS/RANSOMWARE**
NAME	**BAS ATTACKS**	cpe:2.3:a:adobe:flash_player:*:*:*:*:*:*:*:*	-
Adobe Flash Player Code Execution Vulnerability	✗		
	CWE ID	**ASSOCIATED TTPs**	**PATCH LINKS**
	-	T1059: Command and Scripting Interpreter	https://lists.opensuse.org/archives/list/security-announce@lists.opensuse.org/message/D3BYNRD5U4PMJJBKBUXU3VUSOSRUQJZ7/

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2013-0643	✗	Adobe Flash Player before 10.3.183.67 and 11.x before 11.6.602.171 on Windows and Mac OS X, and before 10.3.183.67 and 11.x before 11.2.202.273 on Linux	-
	ZERO-DAY		
	✓	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS	cpe:2.3:a:adobe:flash_player:*:*:*:*:*:*:*:*	-
Adobe Flash Player Incorrect Default Permissions Vulnerability	✗		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-269	T1059: Command and Scripting Interpreter	https://access.redhat.com/errata/RHSA-2013:0574.html , https://lists.opensuse.org/archives/list/security-announce@lists.opensuse.org/message/JIHDCJYZOMKRWAXFWK3OTAKQCUYPFROV/ , https://lists.opensuse.org/archives/list/security-announce@lists.opensuse.org/message/AESHDAQS4OJINLG6LBRZ77TED2XQMDVW/ , https://lists.opensuse.org/archives/list/security-announce@lists.opensuse.org/message/AGBDVPYFSYNAJO7VEUPYDDRP5ZYLOLMV/

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2014-0497	✗	Adobe Flash Player before 11.7.700.261 and 11.8.x through 12.0.x before 12.0.0.44 on Windows and Mac OS X, and before 11.2.202.336 on Linux	-
	ZERO-DAY		
	✓	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS	cpe:2.3:a:adobe:flash_player:*:*:*:*:*:*:*:*:*	-
Adobe Flash Player Integer Underflow Vulnerability	✓		
	CWE ID	ASSOCIATED TTPs	PATCH LINKS
	CWE-191	T1059: Command and Scripting Interpreter	https://access.redhat.com/errata/RHSA-2014:0137 , https://lists.opensuse.org/archives/list/security-announce@lists.opensuse.org/message/FXPJOKVRTQPTEUJIRADYJPTEPZOMAZRJ/ , https://lists.opensuse.org/archives/list/security-announce@lists.opensuse.org/message/N47G3J3ACEZ7DXCDPQCNFTMIZGU3SPGQ/ , https://lists.opensuse.org/archives/list/security-announce@lists.opensuse.org/message/KHT67GVSDD4NEJ6YCTPPO5ZD5OBZAHOG/

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2020-14644	⊗	Oracle WebLogic Server: 12.2.1.3.0, 12.2.1.4.0 and 14.1.1.0.0	-
	ZERO-DAY		
	⊗	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS	cpe:2.3:a:oracle:weblogic_server:*:*:*:*:*:*:*:*	-
Oracle WebLogic Server Remote Code Execution Vulnerability	⊗		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	-	T1059: Command and Scripting Interpreter; T1190: Exploit Public-Facing Application	https://www.oracle.com/security-alerts/cpujul2020.html https://support.oracle.com/rs?type=doc&id=2664876.1

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2022-21445	✗	Oracle Application Development Framework (ADF) Version: 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:application_development_framework:*:*:*:*:*:*:*	-
Oracle ADF Faces Deserialization of Untrusted Data Vulnerability	✗		
	CWE ID	ASSOCIATED TTPs	PATCH LINKS
	CWE-502	T1059: Command and Scripting Interpreter	https://www.oracle.com/security-alerts/cpuapr2022.html https://support.oracle.com/rs?type=doc&id=2853458.2

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2020-0618	✗	Microsoft SQL Server	-
	ZERO-DAY		
	✗	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS	cpe:2.3:a:microsoft:sql_server:-:*:*:*:*:*:*	Mallox Ransomware
Microsoft SQL Server Reporting Services Remote Code Execution Vulnerability	✓		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-502	T1059: Command and Scripting Interpreter	https://msrc.microsoft.com/update-guide/en-US/advisory/CVE-2020-0618

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2024-27348	✗	Apache HugeGraph-Server from version 1.0.0 to before 1.3.0 in Java8 & Java11	-
	ZERO-DAY		
	✗	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS	cpe:2.3:a:apache:hugegraph-server:*:*:*:*:*:*:*:*	-
Apache HugeGraph-Server Improper Access Control Vulnerability	✓		
	CWE ID	ASSOCIATED TTPs	PATCH LINKS
	CWE-77	T1059: Command and Scripting Interpreter, T1190 : Exploit Public-Facing Application	https://hugegraph.apache.org/docs/download/download/

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2024-8963	✗	CSA 4.6 (All versions before Patch 519)	-
	ZERO-DAY		
	✗	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS	cpe:2.3:a:ivanti:endpoint_manager_cloud_services_appliance:4.6:-:*:*:*:*:*:* cpe:2.3:a:ivanti:endpoint_manager_cloud_services_appliance:4.6:patch_512:*:*:*:*:*:*	-
Ivanti Cloud Services Appliance (CSA) Path Traversal Vulnerability	✗		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-22	T1059: Command and Scripting Interpreter	https://forums.ivanti.com/s/article/CSA-5-0-Download , https://forums.ivanti.com/s/article/CSA-4-6-Patch-519

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2024-7593	⊗	Ivanti Virtual Traffic Manager Versions: 22.2, 22.3, 22.3R2, 22.5R1, 22.6R1, 22.7R1	-
	ZERO-DAY		
	⊗	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS	cpe:2.3:a:ivanti:vtm:*:*:*:*:*:*:*	-
Ivanti Virtual Traffic Manager Authentication Bypass Vulnerability	⊗		
	CWE ID	ASSOCIATED TTPs	PATCH LINKS
	CWE-287, CWE-303	T1068: Exploitation for Privilege Escalation; T1556: Modify Authentication Process	https://forums.ivanti.com/s/article/Security-Advisory-Ivanti-Virtual-Traffic-Manager-vTM-CVE-2024-7593?language=en_US

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2019-0344	⊗	SAP Commerce Cloud (virtualjdbc extension), versions 6.4, 6.5, 6.6, 6.7, 1808, 1811, 1905	-
	ZERO-DAY		
	⊗	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS	cpe:2.3:a:sap:commerce_cloud:*:*:*:*:*:*:*	-
SAP Commerce Cloud Deserialization of Untrusted Data Vulnerability	⊗		
	CWE ID	ASSOCIATED TTPs	PATCH LINKS
	CWE-502	T1059: Command and Scripting Interpreter	https://me.sap.com/notes/2786035

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2021-4043	✗	GitHub repository gpac/gpac prior to 1.1.0	-
	ZERO-DAY		
	✗	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS	cpe:2.3:a:gpac:gpac:*:*:*:*:*:*:*:*	-
Motion Spell GPAC Null Pointer Dereference Vulnerability	✓		
	CWE ID	ASSOCIATED TTPs	PATCH LINKS
	CWE-476	T1588.006: Vulnerabilities; T1499: Endpoint Denial of Service	https://github.com/gpac/gpac/commit/64a2e1b799352ac7d7aad1989bc06e7b0f2b01db , https://huntr.com/bounties/d7a534cb-df7a-48ba-8ce3-46b1551a9c47

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2020-15415	✗	DrayTek Vigor3900, Vigor2960, and Vigor300B devices before 1.5.1	-
	ZERO-DAY		
	✗	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS	cpe:2.3:o:draytek:vigor_firmware:*:*:*:*:*:*:*:* cpe:2.3:h:draytek:vigor:-:*:*:*:*:*:*:*	-
DrayTek Multiple Vigor Routers OS Command Injection Vulnerability	✗		
	CWE ID	ASSOCIATED TTPs	PATCH LINKS
	CWE-78	T1059: Command and Scripting Interpreter	https://www.draytek.com/about/security-advisory/vigor3900-/-vigor2960-/-vigor300b-remote-code-injection/execution-vulnerability-(cve-2020-14472)

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2023-25280	⊗	D-Link DIR820LA1_FW105B03	-
	ZERO-DAY		
	⊗	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS	cpe:2.3:o:dlink:dir820la1_firmware:*:*:*:*:*:*:*:*	Mirai botnet
D-Link DIR-820 Router OS Command Injection Vulnerability	⊗		
	CWE ID	ASSOCIATED TTPs	PATCH LINKS
	CWE-78	T1059: Command and Scripting Interpreter	https://github.com/migraine-sudo/D_Link_Vuln/tree/main/cmd%20Inject%20in%20pingV4Msg

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.

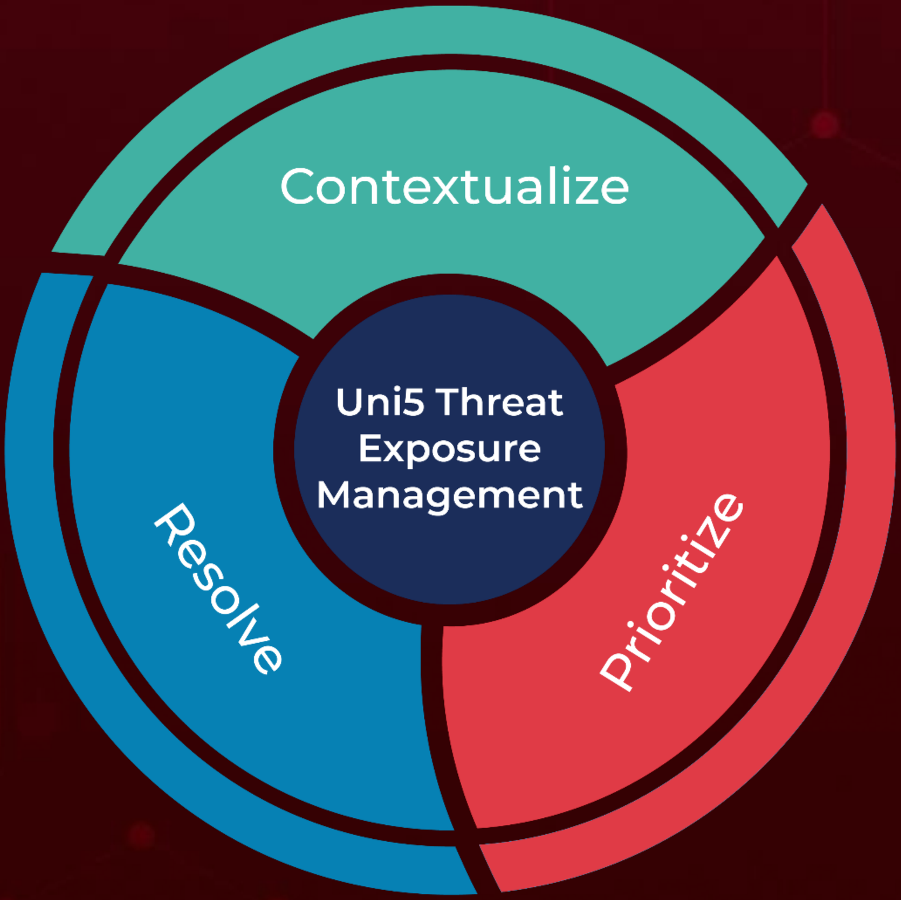
BAS Attacks: “BAS attacks” are the simulated cyber-attacks that can be carried out by our in-house Uni5's Breach and Attack Simulation (BAS), which organizations could use to identify vulnerabilities and improve their overall security posture.

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

October 1, 2024 • 8:30 AM

More at www.hivepro.com