Date of Publication
June 4, 2024

Hive Pro

HiveForce Labs

CISA KNOWN EXPLOITED VULNERABILITY CATALOG

May 2024

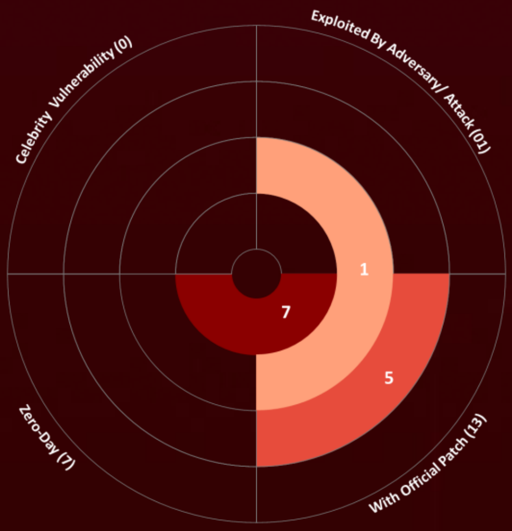
Table of Contents

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 May 2024, fourteen vulnerabilities met the criteria for inclusion in the CISA's KEV catalog. Of these, seven are zero-day vulnerabilities; one has 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-2023-7028	GitLab Community and Enterprise Editions Improper Access Control Vulnerability	GitLab GitLab CE/EE	7.5	✗	✓	May 22, 2024
CVE-2024-4671	Google Chromium Visuals Use-After-Free Vulnerability	Google Chromium	9.6	✓	✓	June 3, 2024
CVE-2024-30040	Microsoft Windows MSHTML Platform Security Feature Bypass Vulnerability	Microsoft Windows	8.8	✓	✓	June 4, 2024
CVE-2024-30051	Microsoft DWM Core Library Privilege Escalation Vulnerability	Microsoft DWM Core Library	7.8	✓	✓	June 4, 2024
CVE-2024-4761	Google Chromium V8 Out-of-Bounds Memory Write Vulnerability	Google Chromium Visuals	8.8	✓	✓	June 6, 2024
CVE-2021-40655	D-Link DIR-605 Router Information Disclosure Vulnerability	D-Link DIR-605 Router	7.5	✗	✗	June 6, 2024
CVE-2014-100005	D-Link DIR-600 Router Cross-Site Request Forgery (CSRF) Vulnerability	D-Link DIR-600 Router	-	✗	✓	June 6, 2024
CVE-2024-4947	Google Chromium V8 Type Confusion Vulnerability	Google Chromium V8	8.8	✓	✓	June 10, 2024

CVE	NAME	AFFECTED PRODUCT	CVSS 3.x SCORE	ZERO-DAY	PATCH	DUE DATE
CVE-2023-43208	NextGen Healthcare Mirth Connect Deserialization of Untrusted Data Vulnerability	NextGen Healthcare Mirth Connect	9.8	✗	✓	June 10, 2024
CVE-2020-17519	Apache Flink Improper Access Control Vulnerability	Apache Flink	7.5	✗	✓	June 13, 2024
CVE-2024-5274	Google Chromium V8 Type Confusion Vulnerability	Google Chromium V8	8.8	✓	✓	June 18, 2024
CVE-2024-4978	Justice AV Solutions (JAVS) Viewer Installer Embedded Malicious Code Vulnerability	Justice AV Solutions Viewer	8.4	✗	✓	June 19, 2024
CVE-2024-1086	Linux Kernel Use-After-Free Vulnerability	Linux Kernel	7.8	✗	✓	June 20, 2024
CVE-2024-24919	Check Point Quantum Security Gateways Information Disclosure Vulnerability	Check Point Quantum Security Gateways	8.6	✓	✓	June 20, 2024

CVEs Details

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2023-7028	✗	Gitlab CE and EE versions 16.1 - 16.1.5, 16.2 - 16.2.8, 16.3 - 16.3.6, 16.4 - 16.4.4, 16.5 - 16.5.5, 16.6 - 16.6.3, 16.7 - 16.7.1	-
	ZERO-DAY		
	✗	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS	cpe:2.3:a:gitlab:gitlab_community_edition:*:*:*:*:*:*:* cpe:2.3:a:gitlab:gitlab_enterprise_edition:*:*:*:*:*:*:*	-
GitLab Community and Enterprise Editions Improper Access Control Vulnerability	✓		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-284	T1068 : Exploitation for Privilege Escalation	https://about.gitlab.com/releases/2024/01/11/critical-security-release-gitlab-16-7-2-released/

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2024-4671	✗	Google Chrome prior to 124.0.6367.201	-
	ZERO-DAY		
	✓	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS	cpe:2.3:a:google:chrome:*:*:*:*:*:*:*	-
Google Chrome Visuals Use After Free Vulnerability	✗		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-416	T1059: Command and Scripting Interpreter; T1189: Drive-by Compromise; T1203: Exploitation for Client Execution	https://www.google.com/intl/en/chrome/?standalone=1

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2024-30040	✗	Microsoft Windows	-
	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 MSHTML Platform Security Feature Bypass Vulnerability	✗		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-20	T1204: User Execution	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-30040

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2024-30051	✗	Microsoft Windows DWM Core Library	-
	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 DWM Core Library Elevation of Privilege Vulnerability	✓		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-122	T1068: Exploitation for Privilege Escalation	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-30051

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2024-4761	✗	Google Chrome	-
	ZERO-DAY		
	✓	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS	cpe:2.3:a:google:chrome:*:*:*:*:*:*:*	-
Google Chrome Out of bounds write in V8 Vulnerability	✓		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-787	T1059.007: JavaScript T1189: Drive by Compromise	https://www.google.com/intl/en/chrome/?standalone=1

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2021-40655	✗	DIR-605: 2.01MT	-
	ZERO-DAY		
	✗	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS	cpe:2.3:o:dlink:dir-605l_firmware:2.01mt:*:*:*:*:*:*:*	-
D-Link DIR-605 Router Information Disclosure Vulnerability	✓		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-863	1190 : Exploit Public-Facing Application, T1082 : System Information Discovery	-

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2014-100005	✗	Dir-600: before 2.17b02	-
	ZERO-DAY		
	✗	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS	cpe:2.3:o:dlink:dir-600_firmware:*:*:*:*:*:*:*:*	-
D-Link DIR-600 Router Cross-Site Request Forgery (CSRF) Vulnerability	✗		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-352	T1059 : Command and Scripting Interpreter, T1068: Exploitation for Privilege Escalation	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10018

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
[CVE-2024-4947]()	✗	Google Chrome	-
	ZERO-DAY		
	✓	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS	cpe:2.3:a:google:chrome:*:*:*:*:*:*:*:*	-
Google Chrome Type Confusion in V8 Vulnerability	✗		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-843	T1059.007: JavaScript T1189: Drive-by Compromise	https://www.google.com/intl/en/chrome/?standalone=1

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2023-43208	✗	NextGen Healthcare Mirth Connect before version 4.4.1	-
	ZERO-DAY		
	✗	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS	cpe:2.3:a:nextgen:mirth_connect:*:*:*:*:*:*:*:*	-
NextGen Healthcare Mirth Connect Deserialization of Untrusted Data Vulnerability	✓		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-502	T1059 : Command and Scripting Interpreter	https://github.com/nextgenhealthcare/connect/wiki/4.4.1---What%27s-New

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2020-17519	✗	Flink: 1.11.0 - 1.11.2	-
	ZERO-DAY		
	✗	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS	cpe:2.3:a:apache:flink:*:*:*:*:*:*:*:*	-
Apache Flink Improper Access Control Vulnerability	✓		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-552	T1068 : Exploitation for Privilege Escalation	https://www.google.com/intl/en/chrome/?standalone=1

<table>
<tr><th>CVE ID</th><th>CELEBRITY VULNERABILITY</th><th>AFFECTED PRODUCTS</th><th>ASSOCIATED ACTOR</th></tr>
<tr><td rowspan="3">CVE-2024-5274</td><td>✗</td><td rowspan="2">Google Chrome</td><td rowspan="2">-</td></tr>
<tr><td><b>ZERO-DAY</b></td></tr>
<tr><td>✓</td><td><b>AFFECTED CPE</b></td><td><b>ASSOCIATED ATTACKS/RANSOMWARE</b></td></tr>
<tr><td><b>NAME</b></td><td><b>BAS ATTACKS</b></td><td rowspan="2">cpe:2.3:a:google:chrome:*:*:*:*:*:*:*</td><td rowspan="2">-</td></tr>
<tr><td rowspan="3">Google Chrome Type Confusion in V8 Vulnerability</td><td>✗</td></tr>
<tr><td><b>CWE ID</b></td><td><b>ASSOCIATED TTPs</b></td><td><b>PATCH LINK</b></td></tr>
<tr><td>CWE-843</td><td>T1059.007: JavaScript, T1203: Exploitation for Client Execution</td><td>https://www.google.com/intl/en/chrome/?standalone=1</td></tr>
</table>

<table>
<tr><th>CVE ID</th><th>CELEBRITY VULNERABILITY</th><th>AFFECTED PRODUCTS</th><th>ASSOCIATED ACTOR</th></tr>
<tr><td rowspan="3">CVE-2024-4978</td><td>✗</td><td rowspan="2">JAVS Viewer software</td><td rowspan="2">-</td></tr>
<tr><td><b>ZERO-DAY</b></td></tr>
<tr><td>✗</td><td><b>AFFECTED CPE</b></td><td><b>ASSOCIATED ATTACKS/RANSOMWARE</b></td></tr>
<tr><td><b>NAME</b></td><td><b>BAS ATTACKS</b></td><td rowspan="2">cpe:2.3:a:justice_av_solutions:viewer:*:*:*:*:*:*:*</td><td rowspan="2">RustDoor, GateDoor</td></tr>
<tr><td rowspan="3">JAVS Arbitrary code Execution Vulnerability</td><td>✓</td></tr>
<tr><td><b>BAS ATTACKS</b></td><td><b>ASSOCIATED TTPs</b></td><td><b>PATCH LINK</b></td></tr>
<tr><td>CWE-506</td><td>T1059: Command and Scripting Interpreter, T1027.009: Embedded Payloads</td><td>https://www.javs.com/downloads/</td></tr>
</table>

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2024-1086	✗	Linux Kernel	-
	ZERO-DAY		
	✗	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS	cpe:2.3:o:linux:linux_kernel:*:*:*:*:*:*:*:*	-
Linux Kernel Use-After-Free Vulnerability	✗		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-416	T1059: Command and Scripting Interpreter; T1189: Drive-by Compromise; T1203: Exploitation for Client Execution	https://git.kernel.org/pub/scm/linux/kernel/git/torvalds/linux.git/commit/?id=f342de4e2f33e0e39165d8639387aa6c19dff660

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2024-24919	✗	Check Point Security Gateway	-
	ZERO-DAY		
	✓	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS	cpe:2.3:a:checkpoint:quantum_gateway:*:*:*:*:*:*	-
Check Point Security Gateway Information Disclosure Vulnerability	✗		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-200	T1133: External Remote Services, T1212: Exploitation for Credential Access	https://support.checkpoint.com/results/sk/sk182336

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.

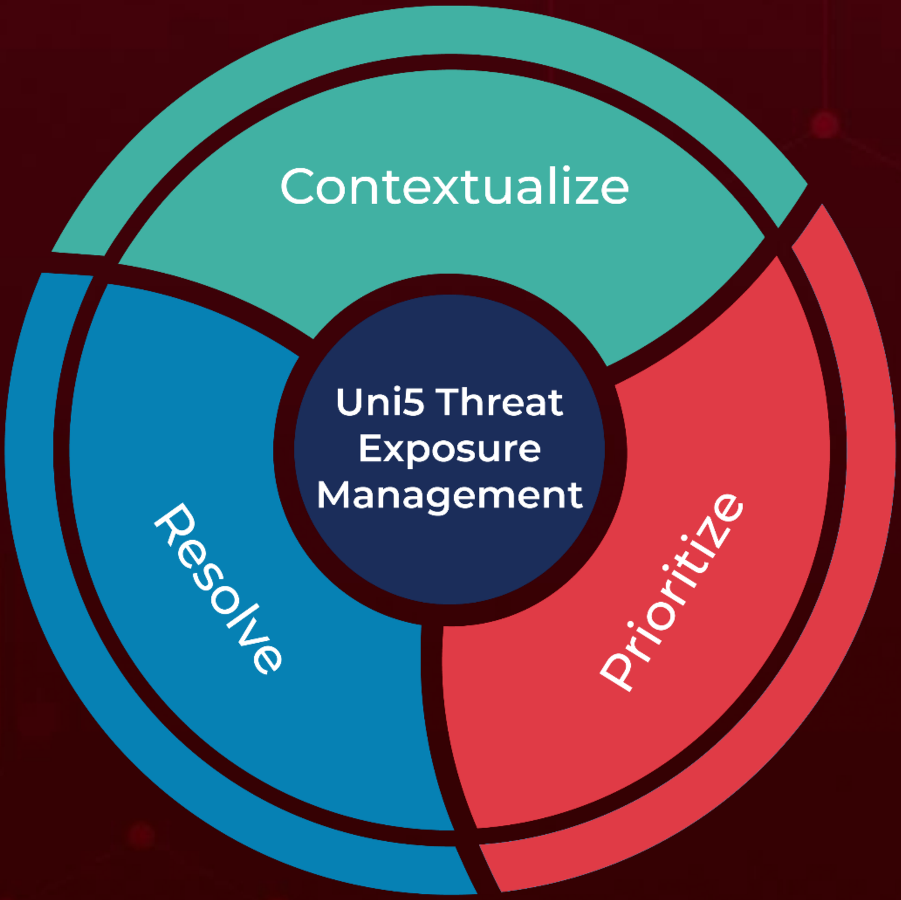
BAS Attacks: “BAS attacks” are the simulated cyber-attacks that can be carried out by our in-house Uni5's Breach and Attack Simulation (BAS), which organizations could use to identify vulnerabilities and improve their overall security posture.

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

June 4, 2024 • 7:30 AM

© 2024 All Rights are Reserved by Hive Pro

More at www.hivepro.com