Date of Publication
July 1, 2024

Hive Pro

HiveForce Labs

CISA KNOWN EXPLOITED VULNERABILITY CATALOG

June 2024

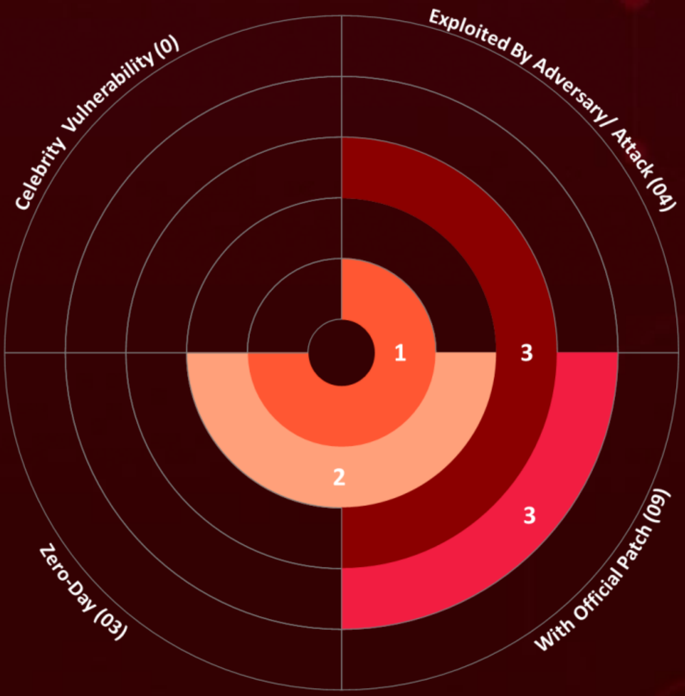
Table of Contents

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

09
Known Exploited Vulnerabilities



CVEs List

CVE	NAME	AFFECTED PRODUCT	CVSS 3.x SCORE	ZERO-DAY	PATCH	DUE DATE
CVE-2017-3506	Oracle WebLogic Server OS Command Injection Vulnerability	Oracle WebLogic Server	7.4	✗	✓	June 24, 2024
CVE-2024-4577	PHP-CGI OS Command Injection Vulnerability	PHP Group PHP	9.8	✗	✓	July 3, 2024
CVE-2024-4610	Arm Mali GPU Kernel Driver Use-After-Free Vulnerability	Arm Mali GPU Kernel Driver	5.5	✓	✓	July 3, 2024
CVE-2024-4358	Progress Telerik Report Server Authentication Bypass by Spoofing Vulnerability	Progress Telerik Report Server	9.8	✗	✓	July 4, 2024
CVE-2024-26169	Microsoft Windows Error Reporting Service Improper Privilege Management Vulnerability	Microsoft Windows	7.8	✓	✓	July 4, 2024
CVE-2024-32896	Google Pixel Privilege Escalation Vulnerability	Google Pixel	7.8	✓	✓	July 4, 2024
CVE-2020-13965	Roundcube Webmail Cross-Site Scripting (XSS) Vulnerability	Roundcube Webmail	6.1	✗	✓	July 17, 2024
CVE-2022-2586	Linux Kernel Use-After-Free Vulnerability	Linux Kernel	7.8	✗	✓	July 17, 2024
CVE-2022-24816	GeoSolutionsGroup JAI-EXT Code Injection Vulnerability	GeoSolutionsGroup JAI-EXT	9.8	✗	✓	July 17, 2024

CVEs Details

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
[CVE-2017-3506](CVE-2017-3506)	✗	Oracle WebLogic Server: 12.1.3.0.0 - 12.2.1.2	8220 Gang
	ZERO-DAY		
	✗	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS	cpe:2.3:a:oracle:oracle_weblogic_server:*:*:*:*:*:*:*:*	-
Oracle WebLogic Server OS Command Injection Vulnerability	✓		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-284	T1498: Network Denial of Service, T1190: Exploit Public-Facing Application	https://www.oracle.com/security-alerts/cpuapr2017.html

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2024-4577	✗	PHP versions: 8.1.* before 8.1.29, 8.2.* before 8.2.20, 8.3.* before 8.3.8	-
	ZERO-DAY		
	✗	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS	cpe:2.3:a:php:php:*:*:*:*:*:*:*:*	TellYouThePass ransomware
PHP-CGI OS Command Injection Vulnerability	✓		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-78	T1059: Command and Scripting Interpreter, T1190: Exploit Public-Facing Application	https://www.php.net/downloads

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2024-4610	✗	Bifrost GPU Kernel Driver: All versions from r34p0 to r40p0Valhall GPU Kernel Driver: All versions from r34p0 to r40p0	-
	ZERO-DAY		
	✓	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS	cpe:2.3:a:arm:bifrost_gpu_kernel_driver:*:*:*:*:*:*:*:* cpe:2.3:a:arm:valhall_gpu_kernel_driver:*:*:*:*:*:*:*:*	-
Arm Mali GPU Kernel Driver Use-After-Free Vulnerability	✗		
	CWE ID	ASSOCIATED TTPs	PATCH LINKS
	CWE-416	T1059: Command and Scripting Interpreter	https://developer.arm.com/downloads/-/mali-drivers/bifrost-kernel https://developer.arm.com/downloads/-/mali-drivers/valhall-kernel

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2024-4358	✗	Progress Telerik Report Server, version 2024 Q1 (10.0.24.305) or earlier	-
	ZERO-DAY		
	✗	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS	cpe:2.3:a:progress:telerik_report_server:*:*:*:*:*:*:*:*	-
Progress Telerik Report Server Authentication Bypass by Spoofing Vulnerability	✓		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-290	T1190: Exploit Public-Facing Application, T1040: Network Sniffing	https://docs.telerik.com/report-server/implementer-guide/setup/upgrade

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2024-26169	✗	Windows: 10 - 11 23H2 Windows Server: 2012 - 2022 23H2	Cardinal Threat Group (aka Storm-1811, UNC4393)
	ZERO-DAY		
	✓	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS	cpe:2.3:o:microsoft:windows:*:*:*:*:*:*:*:*	Black Basta ransomware (aka no_name_software)
Microsoft Windows Error Reporting Service Improper Privilege Management Vulnerability	✓		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-269	T1068: Exploitation for Privilege Escalation	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-26169

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2024-32896	✗	Google Pixel Before 8	-
	ZERO-DAY		
	✓	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS	cpe:2.3:o:google:android:-:*:*:*:*:*:*:*	-
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/2024-06-01

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2020-13965	✗	Roundcube Webmail before 1.3.12 and 1.4.x before 1.4.5	-
	ZERO-DAY		
	✗	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS	cpe:2.3:a:roundcube:webmail:*:*:*:*:*:*:*:*	-
Roundcube Webmail Cross-Site Scripting (XSS) Vulnerability	✗		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-79	T1059: Command and Scripting Interpreter, T1190: Exploit Public-Facing Application	https://roundcube.net/news/2020/06/02/security-updates-1.4.5-and-1.3.12

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2022-2586	✗	Linux Kernel	ExCobalt
	ZERO-DAY		
	✗	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS	cpe:2.3:o:linux:linux_kernel:*:*:*:*:*:*:*:*	GoRed Backdoor
Linux Kernel Use-After-Free Vulnerability	✓		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-416	T1059: Command and Scripting Interpreter	https://lore.kernel.org/netfilter-devel/20220809170148.164591-1-cascardo@canonical.com/T/#t

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2022-24816	☒	GeoSolutionsGroup JAI-EXT before version 1.1.22	-
	ZERO-DAY		
	☒	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS	cpe:2.3:a:geosolutionsgroup:jai-ext:*:*:*:*:*:*:*:*	-
GeoSolutionsGroup JAI-EXT Code Injection Vulnerability	☒		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-94	T1059: Command and Scripting Interpreter, T1190: Exploit Public-Facing Application	https://github.com/geosolutions-it/jai-ext/security/advisories/GHSA-v92f-jx6p-73rx

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.

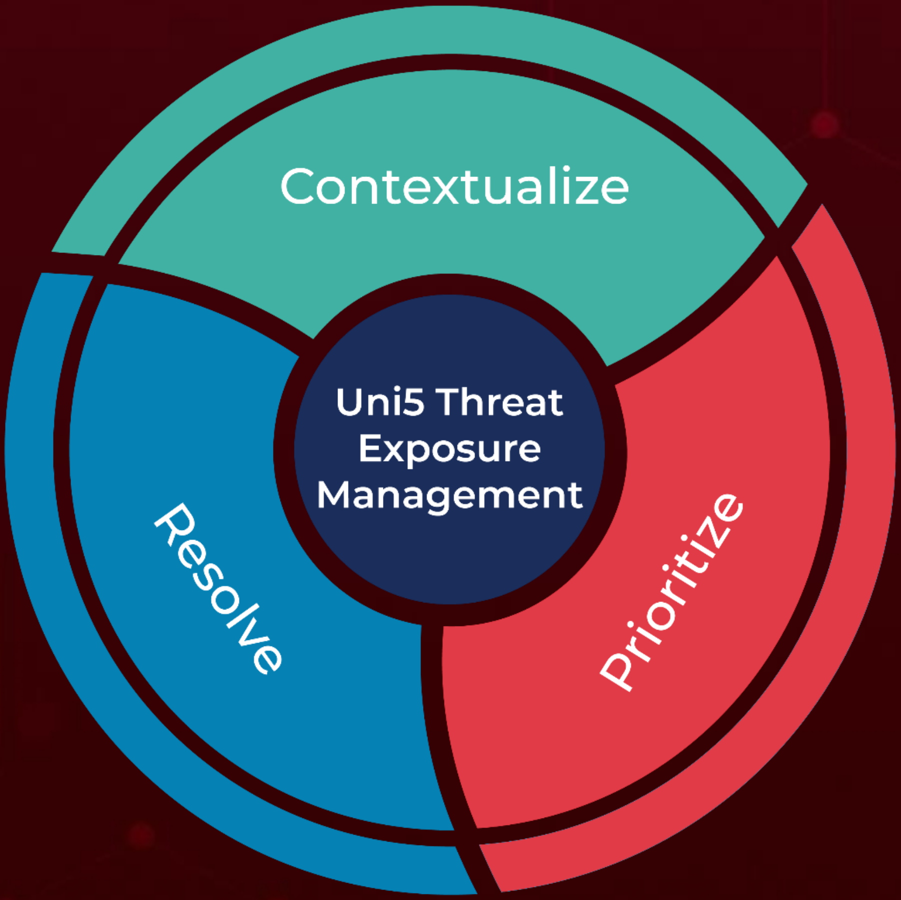
BAS Attacks: “BAS attacks” are the simulated cyber-attacks that can be carried out by our in-house Uni5's Breach and Attack Simulation (BAS), which organizations could use to identify vulnerabilities and improve their overall security posture.

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

July 1, 2024 • 6:00 AM

More at www.hivepro.com