Date of Publication
August 1, 2023

Hive Pro

Hiveforce Labs

CISA KNOWN EXPLOITED VULNERABILITY CATALOG

July 2023

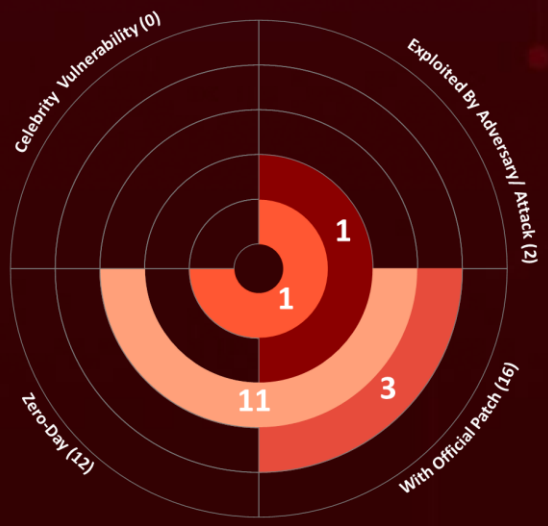
Table of Contents

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 July 2023, sixteen vulnerabilities met the criteria for inclusion in the CISA's KEV catalog. Of these, twelve are zero-day vulnerabilities, and two 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-2021-29256	Arm Mali GPU Kernel Driver Use-After-Free Vulnerability	Arm Mali Graphics Processing Unit (GPU)	8.8	✗	✓	July 28, 2023
CVE-2022-31199	Netwrix Auditor Insecure Object Deserialization Vulnerability	Netwrix Auditor	9.8	✗	✓	Aug 1, 2023
CVE-2023-36874	Microsoft Windows Error Reporting Service Privilege Escalation Vulnerability	Microsoft Windows	7.8	✓	✓	Aug 1, 2023
CVE-2023-35311	Microsoft Outlook Security Feature Bypass Vulnerability	Microsoft Outlook	8.8	✓	✓	Aug 1, 2023
CVE-2023-32049	Microsoft Windows Defender SmartScreen Security Feature Bypass Vulnerability	Microsoft Windows	8.8	✓	✓	Aug 1, 2023
CVE-2023-32046	Microsoft Windows MSHTML Platform Privilege Escalation Vulnerability	Microsoft Windows	7.8	✓	✓	Aug 1, 2023
CVE-2023-37450	Apple Multiple Products WebKit Code Execution Vulnerability	Apple Multiple Products	-	✓	✓	Aug 3, 2023
CVE-2022-29303	SolarView Compact Command Injection Vulnerability	SolarView Compact	9.8	✗	✓	Aug 3, 2023
CVE-2023-36884	Microsoft Office and Windows HTML Remote Code Execution Vulnerability	Microsoft Office and Windows	8.8	✓	✓	Aug 7, 2023
CVE-2023-3519	Citrix NetScaler ADC and NetScaler Gateway Code Injection Vulnerability	Citrix NetScaler ADC and NetScaler Gateway	9.8	✓	✓	Aug 9, 2023

CVE	NAME	AFFECTED PRODUCT	CVSS 3.x SCORE	ZERO-DAY	PATCH	DUE DATE
CVE-2023-38205	Adobe ColdFusion Improper Access Control Vulnerability	Adobe ColdFusion	-	✓	✓	Aug 10, 2023
CVE-2023-29298	Adobe ColdFusion Improper Access Control Vulnerability	Adobe ColdFusion	7.5	✗	✓	Aug 10, 2023
CVE-2023-35078	Ivanti Endpoint Manager Mobile Authentication Bypass Vulnerability	Ivanti Endpoint Manager Mobile (EPMM)	10	✓	✓	Aug 15, 2023
CVE-2023-38606	Apple Multiple Products Kernel Unspecified Vulnerability	Apple Multiple Products	-	✓	✓	Aug 16, 2023
CVE-2023-37580	Zimbra Collaboration (ZCS) Cross-Site Scripting (XSS) Vulnerability	Zimbra Collaboration (ZCS)	-	✓	✓	Aug 17, 2023
CVE-2023-35081	Ivanti Endpoint Manager Mobile (EPMM) Path Traversal Vulnerability	Ivanti Endpoint Manager Mobile (EPMM)	-	✓	✓	Aug 21, 2023

CVEs Details

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2021-29256	✗	Midgard GPU Kernel Driver: before r31p0; Bifrost GPU Kernel Driver: before r30p0; Valhall GPU Kernel Driver: before r30p0	-
	ZERO-DAY		
	✗	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS	cpe:2.3:h:arm:midgard_gpu_kernel_driver:*:*:*:*:*:*:*:*	-
Arm Mali GPU Kernel Driver Use-After-Free Vulnerability	✗		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-416	T1068- Exploitation for Privilege-Escalation	https://developer.arm.com/Arm%20Security%20Center/Mali%20GPU%20Driver%20Vulnerabilities

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2022-31199	✗	Netwrix Auditor: 9.6 - 10.0	-
	ZERO-DAY		
	✗	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS	cpe:2.3:a:netwrix:auditor:10.0:*:*:*:*:*:*:*	Truebot
Netwrix Auditor Insecure Object Deserialization Vulnerability	✓		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-502	T1203: Exploitation for Client Execution	https://security.netwrix.com/Account/SignIn?ReturnUrl=%2FAdvisories%2FADV-2022-003

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2023-36874		Windows: 10 - 11 22H2 Windows Server: 2008 - 2022 20H2	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS	cpe:2.3:o:microsoft:windows:10:1809:*:*:*:*:*:*:*	-
Microsoft Windows Error Reporting Service Privilege Escalation Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH DETAILS
	CWE-119	T1068: Exploitation for Privilege Escalation	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-36874

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2023-35311		Microsoft Office: 2013 - 2019 Microsoft Outlook: 2013 -2016 Microsoft 365 Apps for Enterprise: 32-bit Systems - 64-bit Systems	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS	cpe:2.3:a:microsoft:microsoft_office:2019:*:*:*:*:*:*:*	-
Microsoft Outlook Security Feature Bypass Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH DETAILS
	CWE-254	T1211: Exploitation for Defense Evasion	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35311

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2023-32049		Windows: 10 - 11 22H2 Windows Server: 2016 - 2022 20H2	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS	cpe:2.3:o:microsoft:windows:10:1809:*:*:*:*:*:*	-
Microsoft Windows Defender SmartScreen Security Feature Bypass Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH DETAILS
	CWE-254	T1211: Exploitation for Defense Evasion	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-32049

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2023-32046		Windows: 10 - 11 22H2 Windows Server: 2008 - 2022 20H2 Microsoft Internet Explorer: 11 - 11.1790.17763.0	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS	cpe:2.3:o:microsoft:windows:10:1809:*:*:*:*:*:*	-
Microsoft Windows MSHTML Platform Privilege Escalation Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH DETAILS
	CWE-119	T1068: Exploitation for Privilege Escalation	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-32046

<table>
<tr><th>CVE ID</th><th>CELEBRITY VULNERABILITY</th><th>AFFECTED PRODUCTS</th><th>ASSOCIATED ACTOR</th></tr>
<tr><td rowspan="3">CVE-2023-37450</td><td>  </td><td rowspan="2">Apple Safari up to 16.5.2
Apple iOS and iPadOS up to 16.5.1
Apple macOS up to 13.4.1.</td><td rowspan="2">-</td></tr>
<tr><td>ZERO-DAY</td></tr>
<tr><td>  </td><td>AFFECTED CPE</td><td>ASSOCIATED ATTACKS/RANSOMWARE</td></tr>
<tr><td>NAME</td><td>BAS ATTACKS</td><td rowspan="2">cpe:2.3:a:apple:safari:16.5.0:*:*:*:*:*:*:*
cpe:2.3:a:apple:safari:16.5.1:*:*:*:*:*:*:*
cpe:2.3:a:apple:safari:16.5.2:*:*:*:*:*:*:*
cpe:2.3:o:apple:iphone_os:16.5.0:*:*:*:*:*:*:*
cpe:2.3:o:apple:iphone_os:16.5.1:*:*:*:*:*:*:*
cpe:2.3:o:apple:ipados:16.5.0:*:*:*:*:*:*:*
cpe:2.3:o:apple:mac_os:13.4.0:*:*:*:*:*:*:*
cpe:2.3:o:apple:mac_os:13.4.1:*:*:*:*:*:*:*</td><td rowspan="2">-</td></tr>
<tr><td rowspan="3">Apple WebKit Remote Code Execution Vulnerability</td><td>  </td></tr>
<tr><td>CWE ID</td><td>ASSOCIATED TTPs</td><td>PATCH DETAILS</td></tr>
<tr><td>CWE-94</td><td>T1068- Exploitation for Privilege- Escalation, T1190- Exploit Public-Facing- Application, T1203: Exploitation for Client Execution</td><td>https://support.apple.com/en-gb/HT213826; https://support.apple.com/en-gb/HT213823; https://support.apple.com/en-gb/HT213825</td></tr>
</table>

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2022-29303		SolarView Compact SV-CPT-MC310: before 7.21; SolarView Compact SV-CPT-MC310F: before 7.21	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS	cpe:2.3:h:contec:solarview_compact_sv-cpt-mc310:*:*:*:*:*:*:*:*	-
SolarView Compact Command Injection Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH DETAILS
	CWE-78	T1055: Process Injection, T1190- Exploit Public-Facing-Application	https://jvn.jp/en/vu/JVNVU92327282/

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2023-36884		Windows: 10 - 11 22H2 Windows Server: 2008 - 2022 20H2 Microsoft Office: 2013 - 2019 Microsoft Word: 2013 Service Pack 1 - 2019	Storm-0978 (aka DEV-0978, RomCom)
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS	cpe:2.3:o:microsoft:windows:10:1809:*:*:*:*:*:*:*	RomCom Backdoor
Office and Windows HTML Remote Code Execution Vulnerability			
	CWE ID	ASSOCIATED TTPs	Mitigation DETAILS
	CWE-20	T1203: Exploitation for Client Execution	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-36884

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2023-3519		Citrix NetScaler ADC and NetScaler Gateway	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS	cpe:2.3:a:citrix:adc:*:*:*:*:*:*:*:* cpe:2.3:a:citrix:gateway:*:*:*:*:*:*:*:*	-
Citrix NetScaler ADC and NetScaler Gateway Code Injection Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH DETAILS
	CWE-94	T1059: Command and Scripting Interpreter, T1133: External Remote Service	https://support.citrix.com/article/CTX561482/citrix-adc-and-citrix-gateway-security-bulletin-for-cve20233519-cve20233466-cve20233467

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2023-38205		ColdFusion: 2018 - 2023 Update 2	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS	cpe:2.3:a:adobe:coldfusion:2023:Update 2:*:*:*:*:*:*:*	-
Adobe ColdFusion Improper Access Control Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH DETAILS
	CWE-284	T1562: Impair Defenses, T1005: Data from Local System	https://helpx.adobe.com/security/products/coldfusion/apsb23-47.html

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2023-29298	✗	Adobe ColdFusion	-
	ZERO-DAY		
	✗	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS	cpe:2.3:a:adobe:coldfusion:-:*:*:*:*:*:*:*	-
Adobe ColdFusion Improper Access Control Vulnerability	✗		
	CWE ID	ASSOCIATED TTPs	PATCH DETAILS
	CWE-284	T1562: Impair Defenses, T1005: Data from Local System	https://helpx.adobe.com/security/products/coldfusion/apsb23-40.html

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2023-35078	✗	Ivanti Endpoint Manager Mobile	-
	ZERO-DAY		
	✓	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS	cpe:2.3:o:microsoft:windows:10:1809:*:*:*:*:*:*:*	-
Ivanti Endpoint Manager Mobile Authentication Bypass Vulnerability	✗		
	CWE ID	ASSOCIATED TTPs	PATCH DETAILS
	CWE-119	T1404: Exploitation for Privilege Escalation; T1190: Exploit Public-Facing Application	https://forums.ivanti.com/s/article/CVE-2023-35078-Remote-unauthenticated-API-access-vulnerability?language=en_US

<table>
<tr><th>CVE ID</th><th>CELEBRITY VULNERABILITY</th><th>AFFECTED PRODUCTS</th><th>ASSOCIATED ACTOR</th></tr>
<tr><td rowspan="3">CVE-2023-38606</td><td>  </td><td rowspan="2">iOS version before: 15.7.1.
macOS version: 13.0 22A380 - 13.4.1 22F82, watchOS, tvOS</td><td rowspan="2">-</td></tr>
<tr><td>ZERO-DAY</td></tr>
<tr><td>  </td><td>AFFECTED CPE</td><td>ASSOCIATED ATTACKS/RANSOMWARE</td></tr>
<tr><td>NAME</td><td>BAS ATTACKS</td><td rowspan="2">cpe:2.3:o:apple:mac_os:-:*:*:*:*:*:*:*
cpe:2.3:o:apple:iphone_os:-:*:*:*:*:*:*:*</td><td rowspan="2">-</td></tr>
<tr><td rowspan="2">Apple Multiple Products Kernel Unspecified Vulnerability</td><td>  </td></tr>
<tr><td>CWE ID</td><td>ASSOCIATED TTPs</td><td>PATCH DETAILS</td></tr>
<tr><td>CWE-119</td><td>T1203: Exploitation for Client Execution;
T1059: Command and Scripting Interpreter;
T1068:Exploitation for Privilege Escalation</td><td>https://support.apple.com/en-us/HT213841;
https://support.apple.com/en-us/HT213842;
https://support.apple.com/en-us/HT213843;
https://support.apple.com/en-us/HT213844;
https://support.apple.com/en-us/HT213845;
https://support.apple.com/en-us/HT213846;
https://support.apple.com/en-us/HT213848</td></tr>
</table>

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2023-37580		Zimbra Collaboration: 8.8.15 - 8.8.15 Patch 40	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS	cpe:2.3:a:synacor:zimbra_collaboration:8.8.15:Patch 40:*:*:*:*:*:*:*	-
Zimbra Collaboration (ZCS) Cross-Site Scripting (XSS) Vulnerability			
	CWE ID	ASSOCIATED TTPs	Mitigation DETAILS
	CWE-79	T1190: Exploit Public-Facing Application	https://wiki.zimbra.com/wiki/Zimbra_Releases/8.8.15/P41; https://wiki.zimbra.com/wiki/Security_Center

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2023-35081		Ivanti Endpoint Manager Mobile (formerly MobileIron Core): before 11.10.0.3	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS	cpe:2.3:a:ivanti:mobileiron_core:*:*:*:*:*:*:*:*	-
Ivanti Endpoint Manager Mobile (EPMM) Path Traversal Vulnerability			
	CWE ID	ASSOCIATED TTPs	Mitigation DETAILS
	CWE-22	T1203: Exploitation for Client Execution; T1059: Command and Scripting Interpreter;	https://forums.ivanti.com/s/article/CVE-2023-35081-Arbitrary-File-Write?language=en_US

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 Cybersecurity 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 been branded with catchy names and logos due to their impact on high-profile individuals and celebrities are also referred to as Celebrity Publicized Software Flaws.

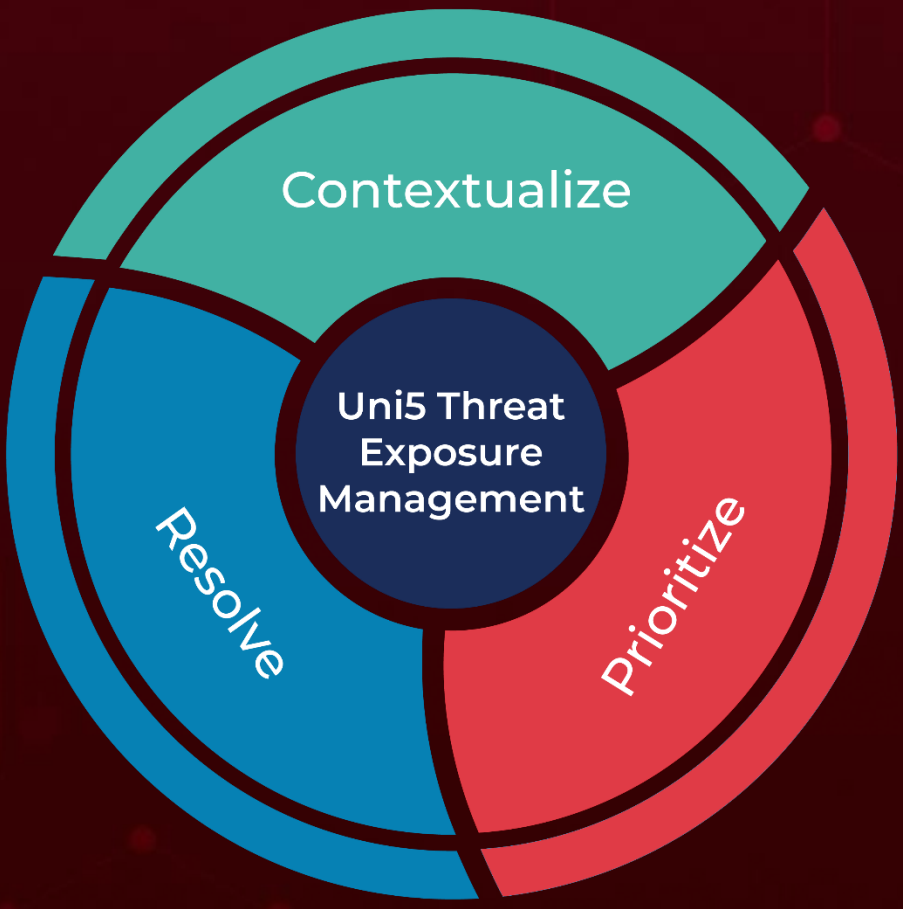
BAS Attacks: “BAS attacks” are the simulated cyber-attacks that can be carried out by our in-house Uni5's Breach and Attack Simulation (BAS), which organizations could use to identify vulnerabilities and improve their overall security posture.

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

August 1, 2023 . 5:30 AM

More at www.hivepro.com