Date of Publication
August 1, 2024

Hive Pro

Hiveforce Labs

CISA KNOWN EXPLOITED VULNERABILITY CATALOG

July 2024

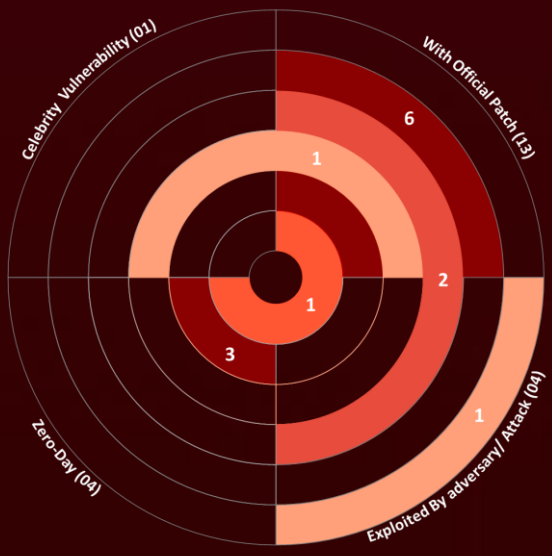
Table of Contents

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 July 2024, fourteen vulnerabilities met the criteria for inclusion in the CISA's KEV catalog. Of these, four are zero-day vulnerabilities; four have 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-2024-20399	Cisco NX-OS Command Injection Vulnerability	Cisco NX-OS	6.7	✓	✓	July 23, 2024
CVE-2024-23692	Rejetto HTTP File Server Improper Neutralization of Special Elements Used in a Template Engine Vulnerability	Rejetto HTTP File Server	9.8	✗	✗	July 30, 2024
CVE-2024-38080	Microsoft Windows Hyper-V Privilege Escalation Vulnerability	Microsoft Windows	7.8	✓	✓	July 30, 2024
CVE-2024-38112	Microsoft Windows MSHTML Platform Spoofing Vulnerability	Microsoft Windows	7.5	✓	✓	July 30, 2024
CVE-2024-36401	OSGeo GeoServer GeoTools Eval Injection Vulnerability	OSGeo GeoServer	9.8	✗	✓	August 5, 2024
CVE-2022-22948	VMware vCenter Server Incorrect Default File Permissions Vulnerability	VMware vCenter Server	6.5	✗	✓	August 7, 2024
CVE-2024-28995	SolarWinds Serv-U Path Traversal Vulnerability	SolarWinds Serv-U	7.5	✗	✓	August 7, 2024
CVE-2024-34102	CosmicSting (Adobe Commerce and Magento Open Source Improper Restriction of XML External Entity Reference (XXE) Vulnerability)	Adobe Commerce and Magento Open Source	9.8	✗	✓	August 7, 2024
CVE-2024-39891	Twilio Authy Information Disclosure Vulnerability	Twilio Authy	5.3	✗	✓	August 13, 2024

CVE	NAME	AFFECTED PRODUCT	CVSS 3.x SCORE	ZERO-DAY	PATCH	DUE DATE
CVE-2012-4792	Microsoft Internet Explorer Use-After-Free Vulnerability	Microsoft Internet Explorer	9.3	✓	✓	August 13, 2024
CVE-2023-45249	Acronis Cyber Infrastructure (ACI) Insecure Default Password Vulnerability	Acronis Cyber Infrastructure (ACI)	9.8	✗	✓	August 19, 2024
CVE-2024-5217	ServiceNow Incomplete List of Disallowed Inputs Vulnerability	ServiceNow Utah, Vancouver, and Washington DC Now	9.2	✗	✓	August 19, 2024
CVE-2024-4879	ServiceNow Improper Input Validation Vulnerability	ServiceNow Utah, Vancouver, and Washington DC Now	9.3	✗	✓	August 19, 2024
CVE-2024-37085	VMware ESXi Authentication Bypass Vulnerability	VMware ESXi	7.2	✗	✓	August 20, 2024

CVEs Details

<table>
<tr><th>CVE ID</th><th>CELEBRITY VULNERABILITY</th><th>AFFECTED PRODUCTS</th><th>ASSOCIATED ACTOR</th></tr>
<tr><td rowspan="3">CVE-2024-20399</td><td>  </td><td rowspan="2">MDS 9000 Series Multilayer Switches
Nexus 3000 Series Switches
Nexus 5500 Platform Switches
Nexus 5600 Platform Switches
Nexus 6000 Series Switches
Nexus 7000 Series Switches
Nexus 9000 Series Switches in standalone NX-OS mode</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:h:cisco:nx-os:*:*:*:*:*:*:*:*</td><td rowspan="2">-</td></tr>
<tr><td rowspan="3">Cisco NX-OS Command Injection Vulnerability</td><td>  </td></tr>
<tr><td>CWE ID</td><td>ASSOCIATED TTPs</td><td>PATCH LINK</td></tr>
<tr><td>CWE-78</td><td>T1059: Command and Scripting Interpreter, T1059.008: Network Device CLI</td><td>https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-cmd-injection-xD9OhyOP#fs</td></tr>
</table>

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2024-23692	✗	Rejetto HTTP File Server up to 2.3m	-
	ZERO-DAY		
	✗	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS	cpe:2.3:a:rejetto:http_file_server:*:*:*:*:*:*:*:*	LemonDuck, GoThief, XenoRAT, Gh0stRAT, and PlugX
Rejetto HTTP File Server Improper Neutralization of Special Elements Used in a Template Engine Vulnerability	✓		
	CWE ID	ASSOCIATED TTPs	PATCH LINKS
	CWE-94 CWE-1336	T1059: Command and Scripting Interpreter	Rejetto HFS 2.3m is no longer supported

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2024-38080	✗	Windows Server: before 2022 10.0.20348.2582 Windows: before 11 23H2 10.0.22631.3880	-
	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 Hyper-V Privilege Escalation Vulnerability	✗		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-190	T1068: Exploitation for Privilege Escalation	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38080

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2024-38112	✗	Microsoft Internet Explorer: 11 - 11.1790.17763.0 Windows: before 11 23H2 10.0.22631.3880 Windows Server: before 2022 10.0.20348.2582	-
	ZERO-DAY		
	✓	**AFFECTED CPE**	**ASSOCIATED ATTACKS/RANSOMWARE**
NAME	**BAS ATTACKS**	cpe:2.3:a:microsoft:internet_explorer:-:*:*:*:*:*:*:* cpe:2.3:o:microsoft:windows:*:*:*:*:*:*:*:* cpe:2.3:o:microsoft:windows_server:*:*:*:*:*:*:*:*	-
Microsoft Windows MSHTML Platform Spoofing Vulnerability	✓		
	CWE ID	**ASSOCIATED TTPs**	**PATCH LINK**
	CWE-668	T1204: User Exécution, T1204.002: Malicious File, T1040 : Network Sniffing	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38112

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2024-36401	✗	OSGeo GeoServer prior to versions 2.23.6, 2.24.4, and 2.25.2	-
	ZERO-DAY		
	✗	**AFFECTED CPE**	**ASSOCIATED ATTACKS/RANSOMWARE**
NAME	**BAS ATTACKS**	cpe:2.3:a:geoserver:geoserver:*:*:*:*:*:*:*:*	-
OSGeo GeoServer GeoTools Eval Injection Vulnerability	✓		
	CWE ID	**ASSOCIATED TTPs**	**PATCH LINK**
	CWE-94 CWE-95	T1190 : Exploit Public-Facing Application, T1059: Command and Scripting Interpreter	https://github.com/geoserver/geoserver/security/advisories/GHSA-6jj6-gm7p-fcvv

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2022-22948	✗	VMware vCenter Server: 6.5 - 7.0.0	UNC3886
	ZERO-DAY		
	✗	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS	cpe:2.3:a:vmware:vcenter_server:-:*:*:*:*:*:*:*	-
VMware vCenter Server Incorrect Default File Permissions Vulnerability	✗		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-276	T1222 : File and Directory Permissions Modification, T1588.006: Vulnerabilities	https://www.vmware.com/security/advisories/VMSA-2022-0009.html

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2024-28995	✗	SolarWinds Serv-U up to 15.4.2 HF 1	-
	ZERO-DAY		
	✗	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS	cpe:2.3:a:solarwinds:serv-u:*:*:*:*:*:*:*:* cpe:2.3:a:solarwinds:serv-u:15.4.2:-:*:*:*:*:*:* cpe:2.3:a:solarwinds:serv-u:15.4.2:hotfix1:*:*:*:*:*:*	-
SolarWinds Serv-U Path Traversal Vulnerability	✓		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-22	T1005: Data from Local System, T1006: Direct Volume Access	https://support.solarwinds.com/SuccessCenter/s/article/Serv-U-15-4-2-Hotfix-2-Release-Notes

<table>
<tr><th>CVE ID</th><th>CELEBRITY VULNERABILITY</th><th>AFFECTED PRODUCTS</th><th>ASSOCIATED ACTOR</th></tr>
<tr><td rowspan="3">CVE-2024-34102</td><td>✓</td><td rowspan="2">Adobe Commerce: Versions before: 2.4.7; 2.4.6-p5; 2.4.5-p7; 2.4.4-p8; 2.4.3-ext-7 ; 2.4.2-ext-7
Magento Open Source: Versions before: 2.4.7; 2.4.6-p5; 2.4.5-p7; 2.4.4-p8
Adobe Commerce Webhooks Plugin: Versions 1.2.0 to 1.4.0</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:adobe:commerce:*:*:*:*:*:*:*:*
cpe:2.3:a:adobe:magento:*:*:open_source:*:*:*
cpe:2.3:a:adobe:commerce_webhooks:*:*:*:*:*:*:*:*:*</td><td rowspan="2">-</td></tr>
<tr><td rowspan="2">CosmicSting (Adobe Commerce and Magento Open Source Improper Restriction of XML External Entity Reference (XXE) Vulnerability)</td><td>✓</td></tr>
<tr><td>CWE ID</td><td>ASSOCIATED TTPs</td><td>PATCH LINK</td></tr>
<tr><td>CWE-611</td><td>T1059 : Command and Scripting Interpreter, T1190 : Exploit Public-Facing Application, T1606: Forge Web Credentials</td><td>https://experienceleague.adobe.com/en/docs/commerce-operations/release/notes/security-patches/2-4-7-patches</td></tr>
</table>

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2024-39891	✗	Twilio Authy Android before 25.1.0 and Authy iOS before 26.1.0	-
	ZERO-DAY		
	✗	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS	cpe:2.3:a:twilio:authy:*:*:*:*:*:*:iphone_os:*:* cpe:2.3:a:twilio:authy_authenticator:*:*:*:*:*:android:*:*	-
Twilio Authy Information Disclosure Vulnerability	✗		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-203	T1190 : Exploit Public-Facing Application, T1082 : System Information Discovery	https://www.twilio.com/en-us/changelog/Security_Alert_Authy_App_Android_iOS

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2012-4792	✗	Microsoft Internet Explorer: 6 - 8	Energetic Bear, APT19
	ZERO-DAY		
	✓	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS	cpe:2.3:a:microsoft:internet_explorer:*:*:*:*:*:*:*:*	Sakula RAT
Microsoft Internet Explorer Use-After-Free Vulnerability	✗		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-399	T1059: Command and Scripting Interpreter; T1189: Drive-by Compromise; T1059.007: JavaScript	https://learn.microsoft.com/en-us/lifecycle/products/internet-explorer-11

<table>
<tr><th>CVE ID</th><th>CELEBRITY VULNERABILITY</th><th>AFFECTED PRODUCTS</th><th>ASSOCIATED ACTOR</th></tr>
<tr><td rowspan="3">CVE-2023-45249</td><td>✕</td><td rowspan="2">Acronis Cyber Infrastructure (ACI) before build 5.0.1-61, Acronis Cyber Infrastructure (ACI) before build 5.1.1-71, Acronis Cyber Infrastructure (ACI) before build 5.2.1-69, Acronis Cyber Infrastructure (ACI) before build 5.3.1-53, Acronis Cyber Infrastructure (ACI) before build 5.4.4-132</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:acronis:cyber_infrastructure:*:*:*:*:*:*:*:*</td><td rowspan="2">-</td></tr>
<tr><td rowspan="3">Acronis Cyber Infrastructure (ACI) Insecure Default Password Vulnerability</td><td>✕</td></tr>
<tr><td>CWE ID</td><td>ASSOCIATED TTPs</td><td>PATCH LINK</td></tr>
<tr><td>CWE-287
CWE-1393</td><td>T1078: Valid Accounts, T1078.001: Default Accounts</td><td>https://security-advisory.acronis.com/advisories/SEC-6452; https://www.acronis.com/en-sg/support/lifecycle/infrastructure/</td></tr>
</table>

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2024-5217	✗ ZERO-DAY	ServiceNow Now Platform	-
	✗	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS	cpe:2.3:a:servicenow:servicenow:*:*:*:*:*:*:*:*	-
ServiceNow Incomplete List of Disallowed Inputs Vulnerability	✗		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-184	T1059: Command and Scripting Interpreter, T1588: Obtain Capabilities	https://support.servicenow.com/kb?id=kb_article_view&sysparm_article=KB1648313

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2024-4879	✗ ZERO-DAY	ServiceNow Now Platform	-
	✗	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS	cpe:2.3:a:servicenow:servicenow:*:*:*:*:*:*:*:*	-
ServiceNow Improper Input Validation Vulnerability	✓		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-1287	T1059: Command and Scripting Interpreter, T1221 : Template Injection, T1190: Exploit Public-Facing Application	https://support.servicenow.com/kb?id=kb_article_view&sysparm_article=KB1645154

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2024-37085	✗	Microsoft Internet Explorer: 6 - 8	Storm-0506, Storm-1175, Octo Tempest, and Manatee Tempest
	ZERO-DAY		
	✗	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS	cpe:2.3:a:microsoft:internet_explorer:*:*:*:*:*:*:*:*	Akira Ransomware, Black Basta Ransomware, Babuk, Lockbit, and Kuiper
VMware ESXi Authentication Bypass Vulnerability	✗		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-287	T1068 : Exploitation for Privilege Escalation, T1136.002 : Domain Account	https://docs.vmware.com/en/VMware-vSphere/8.0/rn/vsphere-esxi-803-release-notes/index.html; https://docs.vmware.com/en/VMware-Cloud-Foundation/5.2/rn/vmware-cloud-foundation-52-release-notes/index.html

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.

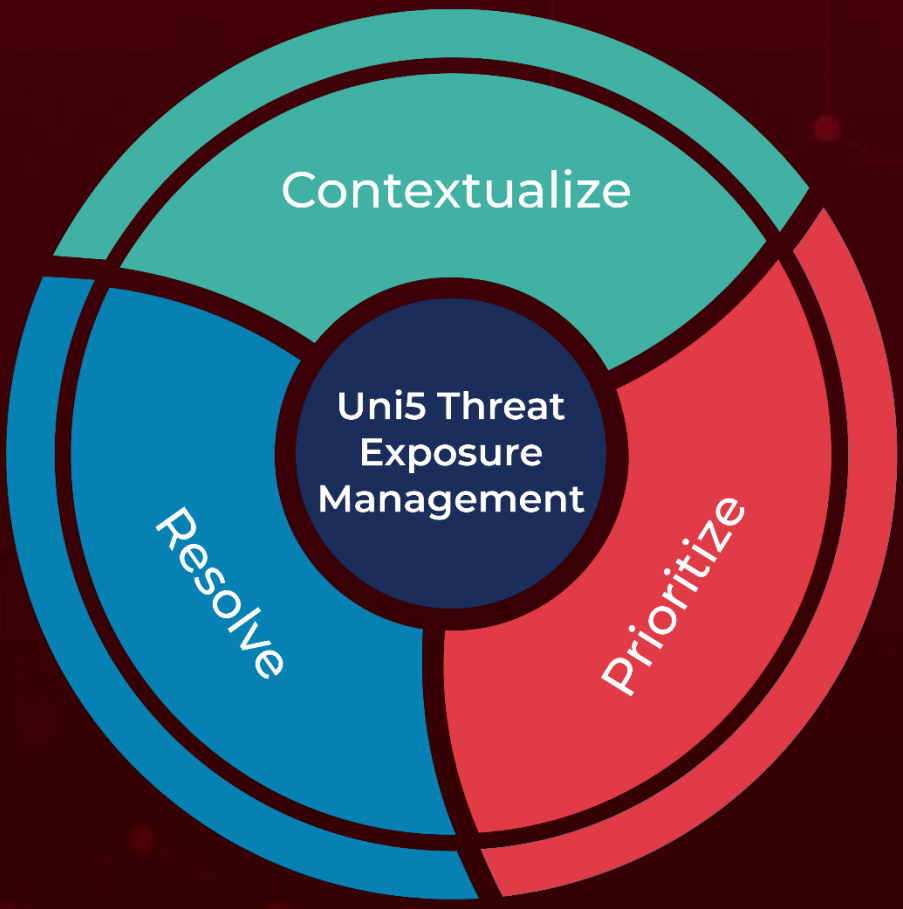
BAS Attacks: “BAS attacks” are the simulated cyber-attacks that can be carried out by our in-house Uni5's Breach and Attack Simulation (BAS), which organizations could use to identify vulnerabilities and improve their overall security posture.

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

August 1, 2024 . 5:00 AM

More at www.hivepro.com