Date of Publication
February 2, 2024

Hive Pro

HiveForce Labs

CISA KNOWN EXPLOITED VULNERABILITY CATALOG

January 2024

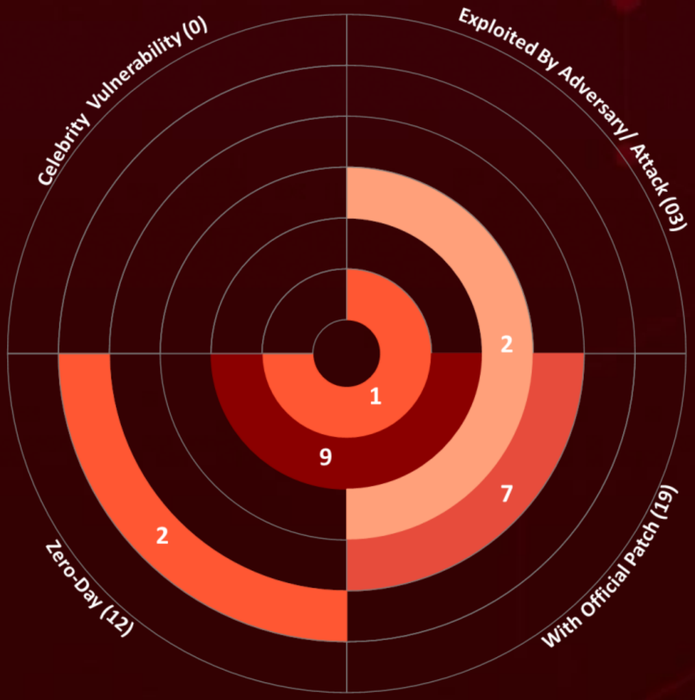
Table of Contents

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

21
Known Exploited Vulnerabilities



CVEs List

CVE	NAME	AFFECTED PRODUCT	CVSS 3.x SCORE	ZERO-DAY	PATCH	DUE DATE
CVE-2023-7101	Spreadsheet::ParseExcel Remote Code Execution Vulnerability	Spreadsheet::ParseExcel	7.8	✓	✓	January 23, 2024
CVE-2023-7024	Google Chromium WebRTC Heap Buffer Overflow Vulnerability	Google Chromium WebRTC	8.8	✓	✓	January 23, 2024
CVE-2023-23752	Joomla! Improper Access Control Vulnerability	Joomla!	5.3	✗	✓	January 29, 2024
CVE-2016-20017	D-Link DSL-2750B Devices Command Injection Vulnerability	D-Link DSL-2750B Devices	9.8	✗	✓	January 29, 2024
CVE-2023-41990	Apple Multiple Products Code Execution Vulnerability	Apple Multiple Products	7.8	✓	✓	January 29, 2024
CVE-2023-27524	Apache Superset Insecure Default Initialization of Resource Vulnerability	Apache Superset	9.8	✗	✓	January 29, 2024
CVE-2023-29300	Adobe ColdFusion Deserialization of Untrusted Data Vulnerability	Adobe ColdFusion	9.8	✗	✓	January 29, 2024
CVE-2023-38203	Adobe ColdFusion Deserialization of Untrusted Data Vulnerability	Adobe ColdFusion	9.8	✗	✓	January 29, 2024
CVE-2023-29357	Microsoft SharePoint Server Privilege Escalation Vulnerability	Microsoft SharePoint Server	9.8	✗	✓	January 31, 2024
CVE-2023-46805	Ivanti Connect Secure and Policy Secure Authentication Bypass Vulnerability	Ivanti Connect Secure and Policy Secure	8.2	✓	✗	January 22, 2024

CVE	NAME	AFFECTED PRODUCT	CVSS 3.x SCORE	ZERO -DAY	PATCH	DUE DATE
CVE-2024-21887	Ivanti Connect Secure and Policy Secure Command Injection Vulnerability	Ivanti Connect Secure and Policy Secure	9.1	✓	✗	January 22, 2024
CVE-2018-15133	Laravel Deserialization of Untrusted Data Vulnerability	Laravel Framework	8.1	✗	✓	February 6, 2024
CVE-2024-0519	Google Chromium V8 Out-of-Bounds Memory Access Vulnerability	Google Chromium V8	8.8	✓	✓	February 7, 2024
CVE-2023-6549	Citrix NetScaler ADC and NetScaler Gateway Buffer Overflow Vulnerability	Citrix NetScaler ADC and NetScaler Gateway	7.5	✓	✓	February 7, 2024
CVE-2023-6548	Citrix NetScaler ADC and NetScaler Gateway Code Injection Vulnerability	Citrix NetScaler ADC and NetScaler Gateway	8.8	✓	✓	January 24, 2024
CVE-2023-35082	Ivanti Endpoint Manager Mobile (EPMM) and MobileIron Core Authentication Bypass Vulnerability	Ivanti Endpoint Manager Mobile (EPMM) and MobileIron Core	9.8	✗	✓	February 8, 2024
CVE-2023-34048	VMware vCenter Server Out-of-Bounds Write Vulnerability	VMware vCenter Server	9.8	✓	✓	February 12, 2024
CVE-2024-23222	Apple Multiple Products Type Confusion Vulnerability	Apple Multiple Products	8.8	✓	✓	February 13, 2024
CVE-2023-22527	Atlassian Confluence Data Center and Server Template Injection Vulnerability	Atlassian Confluence Data Center and Server	9.8	✗	✓	February 14, 2024
CVE-2022-48618	Apple Multiple Products Improper Authentication Vulnerability	Apple Multiple Products	7.8	✓	✓	February 21, 2024
CVE-2024-21893	Ivanti Connect Secure, Policy Secure, and Neurons Server-Side Request Forgery (SSRF) Vulnerability	Ivanti Connect Secure, Policy Secure, and Neurons	8.2	✓	✓	February 2, 2024

CVEs Details

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2023-7101	✗	Spreadsheet::ParseExcel version 0.65	UNC4841
	ZERO-DAY		
	✓	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS	cpe:2.3:a:douglas_wilson:spreadsheet_parseexcel:0.65:*:*:*:*:*:*:*	SEASPY and SALTWATER
Spreadsheet::ParseExcel Remote Code Execution Vulnerability	✗		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-94 CWE-95	T1059: Command and Scripting Interpreter	https://www.barracuda.com/company/legal/esg-vulnerability https://status.barracuda.com/

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2023-7024	✗	Google Chrome: 100.0.4896.60 - 120.0.6099.110	-
	ZERO-DAY		
	✓	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS	cpe:2.3:a:google:chrome:*:*:*:*:*:*:*:*	-
Google Chromium WebRTC Heap Buffer Overflow Vulnerability	✗		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-787	T1574: Hijack Execution Flow	https://www.google.com/intl/en/chrome/?standalone=1

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2023-23752	✗	Joomla!: 4.0.0 - 4.2.7	GambleForce (aka EagleStrike)
	ZERO-DAY		
	✗	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS	cpe:2.3:a:joomla:joomla\!:*:*:*:*:*:*:*:*	-
Joomla! Improper Access Control Vulnerability	✗		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-284	T1059: Command and Scripting Interpreter, T1562: Impair Defenses	https://downloads.joomla.org/

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2016-20017	✗	DSL-2750B: before 1.05	-
	ZERO-DAY		
	✗	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS	cpe:2.3:o:dlink:dsl-2750b_firmware:*:*:*:*:*:*:*:*	-
D-Link DSL-2750B Devices Command Injection Vulnerability	✓		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-77	T1059: Command and Scripting Interpreter	https://supportannouncement.us.dlink.com/announcement/publication.aspx?name=SAP10088

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2023-41990	✗	iOS released before iOS 15.7.1.	-
	ZERO-DAY		
	✓	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS	cpe:2.3:o:apple:ipados:*:*:*:*:*:*:*:* cpe:2.3:o:apple:iphone_os:*:*:*:*:*:*:*:* cpe:2.3:o:apple:macos:*:*:*:*:*:*:*:* cpe:2.3:o:apple:macos:*:*:*:*:*:*:*:*	-
Apple Multiple Products Code Execution Vulnerability	✗		
	CWE ID	ASSOCIATED TTPs	PATCH LINKS
	CWE-77	T1059: Command and Scripting Interpreter, T1658: Exploitation for Client Execution	https://support.apple.com/en-us/HT213599, https://support.apple.com/en-us/HT213601, https://support.apple.com/en-us/HT213605, https://support.apple.com/en-us/HT213606, https://support.apple.com/en-us/HT213842, https://support.apple.com/en-us/HT213844, https://support.apple.com/en-us/HT213845

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2023-27524	⊗	Apache Superset	-
	ZERO-DAY		
	⊗	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS	cpe:2.3:a:apache:superset:*:*:*:*:*:*:*:*	-
Apache Superset Insecure Default Initialization of Resource Vulnerability	⊗		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-1188	T1563: Remote Service Session Hijacking	https://lists.apache.org/thread/n0ftx60sllf527j7g11kmt24wvof8xyk

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2023-29300	⊗	Adobe ColdFusion 2018: Update 17 and earlier Versions, Adobe ColdFusion 2021:Update 7 and earlier Versions,Adobe ColdFusion 2023: Update 1 and earlier versions	-
	ZERO-DAY		
	⊗	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS	cpe:2.3:a:adobe:coldfusion:2023:*:*:*:*:*:*:*	-
Adobe ColdFusion Deserialization of Untrusted Data Vulnerability	⊗		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-502	T1059: Command and Scripting Interpreter	https://helpx.adobe.com/security/products/coldfusion/apsb23-40.html

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2023-38203	⊗	Adobe ColdFusion 2018: Update 17 and earlier Versions,Adobe ColdFusion 2021:Update 7 and earlier Versions,Adobe ColdFusion 2023:Update 1 and earlier versions	-
	ZERO-DAY		
	⊗	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS	cpe:2.3:a:adobe:coldfusion:2023:Update1:*:*:*:*:*:*	-
Adobe ColdFusion Deserialization of Untrusted Data Vulnerability	⊗		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-502	T1059: Command and Scripting Interpreter	https://helpx.adobe.com/security/products/coldfusion/apsb23-41.html

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2023-29357	⊗	Microsoft SharePoint Server: 2019	-
	ZERO-DAY		
	⊗	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS	cpe:2.3:a:microsoft:sharepoint_server:2019:*:*:*:*:*:*:*	-
Microsoft SharePoint Server Privilege Escalation Vulnerability	⊗		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-287	T1068: Exploitation for Privilege Escalation, T1204.001: User Execution	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-29357

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2023-46805	✗	Ivanti Pulse Connect Secure: 9.x and 22.x Ivanti Pulse Policy Secure: 9.x and 22.x	-
	ZERO-DAY		
	✓	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS	cpe:2.3:a:ivanti:connect_secure:*:*:*:*:*:*:*:* cpe:2.3:a:ivanti:policy_secure:*:*:*:*:*:*:*:*	-
Ivanti Connect Secure and Policy Secure Authentication Bypass Vulnerability	✗		
	CWE ID	ASSOCIATED TTPs	MITIGATION LINK
	CWE-287	T1190: Exploit Public-Facing Application, T1040: Network Sniffing	https://forums.ivanti.com/s/article/KB-CVE-2023-46805-Authentication-Bypass-CVE-2024-21887-Command-Injection-for-Ivanti-Connect-Secure-and-Ivanti-Policy-Secure-Gateways?language=en_US

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2018-15133	✗	Laravel Framework through 5.5.40 and 5.6.x through 5.6.29	-
	ZERO-DAY		
	✗	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS	cpe:2.3:a:laravel:laravel:*:*:*:*:*:*:*:*	Androxgh0st
Laravel Deserialization of Untrusted Data Vulnerability	✓		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-502	T1059: Command and Scripting Interpreter	https://laravel.com/docs/5.6/upgrade#upgrade-5.6.30

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2024-21887	✗	Ivanti Pulse Connect Secure: 9.x and 22.x Ivanti Pulse Policy Secure: 9.x and 22.x	-
	ZERO-DAY		
	✓	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS	cpe:2.3:a:ivanti:connect_secure:*:*:*:*:*:*:*:* cpe:2.3:a:ivanti:policy_secure:*:*:*:*:*:*:*:*	-
Ivanti Connect Secure and Policy Secure Command Injection Vulnerability	✓		
	CWE ID	ASSOCIATED TTPs	MITIGATION LINK
	CWE-78	T1059: Command and Scripting Interpreter	https://forums.ivanti.com/s/article/KB-CVE-2023-46805-Authentication-Bypass-CVE-2024-21887-Command-Injection-for-Ivanti-Connect-Secure-and-Ivanti-Policy-Secure-Gateways?language=en_US

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2024-0519	✗	Google Chrome prior to 120.0.6099.224	-
	ZERO-DAY		
	✓	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS	cpe:2.3:a:google:chrome:*:*:*:*:*:*:*:*	-
Google Chromium V8 Out-of-Bounds Memory Access Vulnerability	✗		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-125	T1574: Hijack Execution Flow, T1498: Network Denial of Service	https://www.google.com/intl/en/chrome/?standalone=1

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2023-6549	✗	NetScaler ADC and NetScaler Gateway 14.1 before 14.1-12.35,NetScaler ADC and NetScaler Gateway 13.1 before 13.1-51.15,NetScaler ADC and NetScaler Gateway 13.0 before 13.0-92.21,NetScaler ADC 13.1-FIPS before 13.1-37.176, NetScaler ADC 12.1-FIPS before 12.1-55.302, NetScaler ADC 12.1-NDcPP before 12.1-55.302	-
	ZERO-DAY		
	✓	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS	cpe:2.3:a:citrix:netscaler_ADC_and_Gateway:*:*:*:*:*:*:*	-
Citrix NetScaler ADC and NetScaler Gateway Buffer Overflow Vulnerability	✗		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-119	T1574: Hijack Execution Flow, T1499: Endpoint Denial of Service, T1548: Abuse Elevation Control Mechanism	https://www.citrix.com/downloads/

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2023-6548	✗	NetScaler ADC and NetScaler Gateway 14.1 before 14.1-12.35,NetScaler ADC and NetScaler Gateway 13.1 before 13.1-51.15,NetScaler ADC and NetScaler Gateway 13.0 before 13.0-92.21,NetScaler ADC 13.1-FIPS before 13.1-37.176, NetScaler ADC 12.1-FIPS before 12.1-55.302, NetScaler ADC 12.1-NDcPP before 12.1-55.302	-
	ZERO-DAY		
	✓	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS	cpe:2.3:a:citrix:netscaler_ADC_and_Gateway:*:*:*:*:*:*:*:*	-
Citrix NetScaler ADC and NetScaler Gateway Code Injection Vulnerability	✗		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-94	T1059: Command and Scripting Interpreter	https://www.citrix.com/downloads/

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2023-34048	✗	vCenter Server: 7.0-7.0U3n 8.0- 8.0UIc, VMware Cloud Foundation 5.x, 4.x	-
	ZERO-DAY		
	✓	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS	cpe:2.3:a:vmware:vcenter-server:8.0:U1c:*:*:*:*:*:*	-
VMware vCenter Server Out-of-Bounds Write Vulnerability	✓		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-787	T1588: Obtain Capabilities, T1005: Data from Local System	https://www.vmware.com/security/advisories/VMSA-2023-0023.html

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2023-35082	✗	Ivanti EPMM 11.10 and older	-
	ZERO-DAY		
	✗	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS	cpe:2.3:a:ivanti:endpoint_manager_mobile:*:*:*:*:*:*:*:*	-
Ivanti Endpoint Manager Mobile (EPMM) and MobileIron Core Authentication Bypass Vulnerability	✗		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-287	T1190: Exploit Public-Facing Application, T1040: Network Sniffing	https://forums.ivanti.com/s/article/CVE-2023-35082-Remote-Unauthenticated-API-Access-Vulnerability-in-MobileIron-Core-11-2-and-older?language=en_US

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2022-48618	✗	iOS released before iOS 15.7.1.	-
	ZERO-DAY		
	✓	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS	cpe:2.3:o:apple:ipados:*:*:*:*:*:*:*:*	-
Apple Multiple Products Improper Authentication Vulnerability	✗		
	CWE ID	ASSOCIATED TTPs	PATCH LINKS
	CWE-287	T1078: Valid Accounts, T1040: Network Sniffing	https://support.apple.com/en-us/HT213530, https://support.apple.com/en-us/HT213532, https://support.apple.com/en-us/HT213535, https://support.apple.com/en-us/HT213536

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2024-23222	✗	iPhone, iPad, tvOS, Safari and Mac running macOS Monterey, Ventura, Sonoma	-
	ZERO-DAY		
	✓	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS	cpe:2.3:o:apple:macos:*:*:*:*:*:*:*:* cpe:2.3:a:apple:tvos:*:*:*:*:*:*:*:* cpe:2.3:o:apple:ipados:*:*:*:*:*:*:*:* cpe:2.3:o:apple:iphone_os:*:*:*:*:*:*:*:* cpe:2.3:a:apple:safari:*:*:*:*:*:*:*:*	-
Apple Multiple Products Type Confusion Vulnerability	✗		
	CWE ID	ASSOCIATED TTPs	PATCH LINKS
	CWE-843	T1059: Command and Scripting Interpreter	https://support.apple.com/en-us/HT214055, https://support.apple.com/en-us/HT214056, https://support.apple.com/en-us/HT214057, https://support.apple.com/en-us/HT214058, https://support.apple.com/en-us/HT214059, https://support.apple.com/en-us/HT214060, https://support.apple.com/en-us/HT214061, https://support.apple.com/en-us/HT214063

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2023-22527	✗	Atlassian Confluence Data Center and Server: 8.0.x,8.1.x,8.2.x,8.3.x,8.4.x,8.5.0-8.5.3	-
	ZERO-DAY		
	✗	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS	cpe:2.3:a:atlassian:confluence_data_center:*:*:*:*:*:*:*:* cpe:2.3:a:atlassian:confluence_server:*:*:*:*:*:*:*:*	-
Atlassian Confluence Data Center and Server Template Injection Vulnerability	✗		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-94	T1059: Command and Scripting Interpreter, T1584: Compromise Infrastructure	https://confluence.atlassian.com/security/cve-2023-22527-rce-remote-code-execution-vulnerability-in-confluence-data-center-and-confluence-server-1333990257.html

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2024-21893	✗	Ivanti Connect Secure: 9.x, 22.x and Ivanti Policy Secure: 9.x, 22.x	-
	ZERO-DAY		
	✓	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS	cpe:2.3:a:ivanti:connect_secure:9.0:-:*:*:*:*:*:*	-
Ivanti Connect Secure, Policy Secure, and Neurons Server-Side Request Forgery (SSRF) Vulnerability	✗		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-918	T1090: Proxy, T1135: Network Share Discovery, T1005: Data from Local System, T1133: External Remote Service	https://forums.ivanti.com/s/article/CVE-2024-21888-Privilege-Escalation-for-Ivanti-Connect-Secure-and-Ivanti-Policy-Secure?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 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.

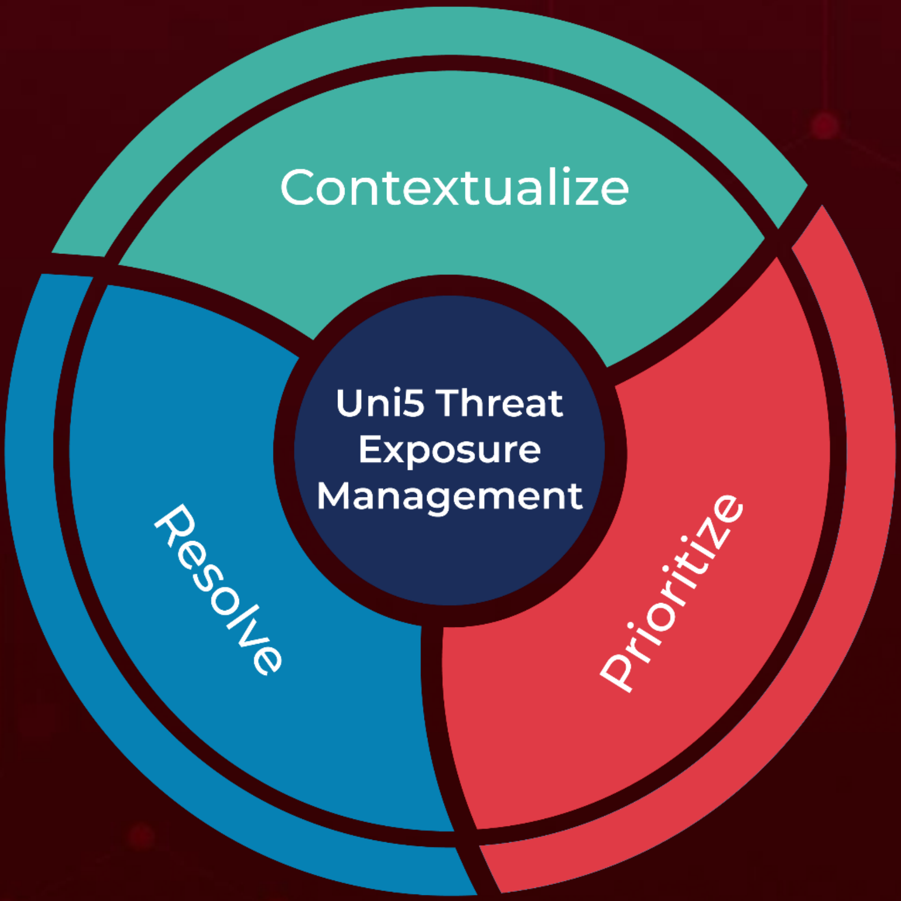
BAS Attacks: “BAS attacks” are the simulated cyber-attacks that can be carried out by our in-house Uni5's Breach and Attack Simulation (BAS), which organizations could use to identify vulnerabilities and improve their overall security posture.

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

February 2, 2024 • 1:30 AM

More at www.hivepro.com