

Date of Publication
November 11, 2024

Hive Pro

HiveForce Labs

CISA

KNOWN

EXPLOITED

VULNERABILITY

CATALOG

October 2024

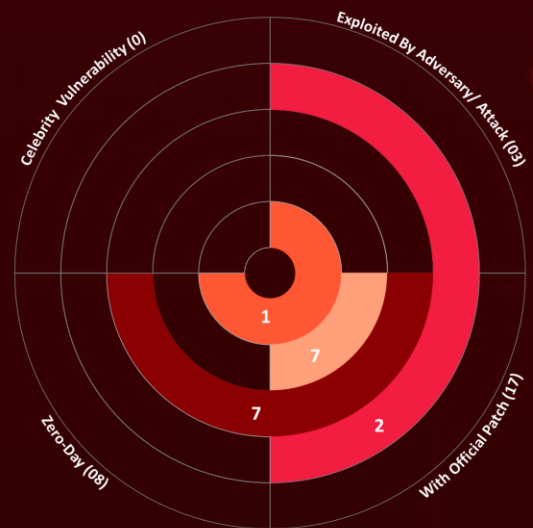
Table of Contents

<u>Summary</u>	03
<u>CVEs List</u>	04
<u>CVEs Details</u>	06
<u>Recommendations</u>	18
<u>References</u>	19
<u>Appendix</u>	19
<u>What Next?</u>	20

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











CVEs List




CVE	NAME	AFFECTED PRODUCT	CVSS 3.x SCORE	ZERO-DAY	PATCH	DUE DATE
CVE-2024-37383	RoundCube Webmail Cross-Site Scripting (XSS) Vulnerability	RoundCube Webmail	6.1			November 14, 2024
CVE-2024-20481	Cisco ASA and FTD Denial-of-Service Vulnerability	Cisco Adaptive Security Appliance (ASA) and Firepower Threat Defense (FTD)	5.8			November 14, 2024
CVE-2024-47575	Fortinet FortiManager Missing Authentication Vulnerability	Fortinet FortiManager	9.8			November 13, 2024
CVE-2024-38094	Microsoft SharePoint Deserialization Vulnerability	Microsoft SharePoint	7.2			November 12, 2024
CVE-2024-9537	ScienceLogic SL1 Unspecified Vulnerability	ScienceLogic SL1	9.8			November 11, 2024
CVE-2024-40711	Veeam Backup and Replication Deserialization Vulnerability	Veeam Backup & Replication	9.8			November 7, 2024
CVE-2024-28987	SolarWinds Web Help Desk Hardcoded Credential Vulnerability	SolarWinds Web Help Desk	9.1			November 5, 2024
CVE-2024-9680	Mozilla Firefox Use-After-Free Vulnerability	Mozilla Firefox	9.8			November 5, 2024
CVE-2024-30088	Microsoft Windows Kernel TOCTOU Race Condition Vulnerability	Microsoft Windows	7.0			November 5, 2024
CVE-2024-9380	Ivanti Cloud Services Appliance (CSA) OS Command Injection Vulnerability	Ivanti Cloud Services Appliance (CSA)	7.2			October 30, 2024




CVE	NAME	AFFECTED PRODUCT	CVSS 3.x SCORE	ZERO-DAY	PATCH	DUE DATE
CVE-2024-9379	Ivanti Cloud Services Appliance (CSA) SQL Injection Vulnerability	Ivanti Cloud Services Appliance (CSA)	7.2			October 30, 2024
CVE-2024-23113	Fortinet Multiple Products Format String Vulnerability	Fortinet Multiple Products	9.8			October 30, 2024
CVE-2024-43573	Microsoft Windows MSHTML Platform Spoofing Vulnerability	Microsoft Windows	8.1			October 29, 2024
CVE-2024-43572	Microsoft Windows Management Console Remote Code Execution Vulnerability	Microsoft Windows	7.8			October 29, 2024
CVE-2024-43047	Qualcomm Multiple Chipsets Use-After-Free Vulnerability	Qualcomm Multiple Chipsets	7.8			October 29, 2024
CVE-2024-45519	Synacor Zimbra Collaboration Command Execution Vulnerability	Synacor Zimbra Collaboration	9.8			October 24, 2024
CVE-2024-29824	Ivanti Endpoint Manager (EPM) SQL Injection Vulnerability	Ivanti Endpoint Manager (EPM)	8.8			October 23, 2024




CVEs Details

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2024-37383		Roundcube Webmail versions before 1.5.7 and Roundcube Webmail versions before 1.6.7	-
	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, T1059.007: JavaScript, T1204: User Execution, T1114.002: Remote Email Collection	Roundcube Webmail version: 1.5.7 and 1.6.7

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
<u>CVE-2024-20481</u>		Cisco Adaptive Security Appliance Cisco Firepower Threat Defense Software	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS	cpe:2.3:a:cisco:adaptive_security_appliance:*:*:*:*:*:*:*	
Cisco ASA and FTD Denial-of-Service Vulnerability		cpe:2.3:a:cisco:firepower_threat_defense_software:*:*:*:*:*:*:*	-
	CWE ID	ASSOCIATED TTPs	PATCH LINKS
	CWE-772	T1574: Hijack Execution Flow, T1499: Endpoint Denial of Service, T1499.004: Application or System Exploitation	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-bf-dos-vDZhLqrW




CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
<u>CVE-2024-47575</u>		FortiManager 7.6.0, FortiManager 7.4.0 through 7.4.4, FortiManager 7.2.0 through 7.2.7, FortiManager 7.0.0 through 7.0.12, FortiManager 6.4.0 through 6.4.14, FortiManager 6.2.0 through 6.2.12, FortiManager Cloud 7.4.1 through 7.4.4, FortiManager Cloud 7.2.1 through 7.2.7, FortiManager Cloud 7.0.1 through 7.0.12, FortiManager Cloud 6.4 (all versions)	UNC5820
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOM WARE
NAME	BAS ATTACKS	cpe:2.3:o:fortinet:fortimanager:*:*:*:*:*:*	-
Fortinet FortiManager Missing Authentication Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-306	T1059: Command and Scripting Interpreter, T1190: Exploit Public-Facing Application	https://fortiguard.com/psirt/FG-IR-24-423




CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
<u>CVE-2024-38094</u>		Microsoft SharePoint	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS	cpe:2.3:a:microsoft:sharepoint_server:-:*:*:*:subscription:*:*:* cpe:2.3:a:microsoft:sharepoint_server:2016:*:*:*:enterprise:*:*:* cpe:2.3:a:microsoft:sharepoint_server:2019:*:*:*:*:*:*	-
Microsoft SharePoint Deserialization Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINKS
	CWE-502	T1190: Exploit Public-Facing Application, T1059: Command and Scripting Interpreter	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38094




CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
<u>CVE-2024-9537</u>		ScienceLogic SL1 versions prior to 12.1.3 ScienceLogic SL1 versions prior to 12.2.3 ScienceLogic SL1 versions prior to 12.3 ScienceLogic SL1 versions prior to 10.1.x ScienceLogic SL1 versions prior to 10.2.x ScienceLogic SL1 versions prior to 11.1.x ScienceLogic SL1 versions prior to 11.2.x ScienceLogic SL1 versions prior to 11.3.x	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS	cpe:2.3:a:sciencelogic:sl1:*:*:*:*:*:*	-
ScienceLogic SL1 Unspecified Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-829	T1059: Command and Scripting Interpreter, T1190: Exploit Public-Facing Application, T1068: Exploitation for Privilege Escalation	https://docs.sciencelogic.com/latest/Content/Web_Admin_and_Accounts/System_Administration/system_admin_system_upgrade.htm




CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
<u>CVE-2024-40711</u>		Veeam Backup & Replication before 12.2.0.334 versions	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS	cpe:2.3:a:veeam:veeam_backup_&_replication:*.~.*.*.*.*.*.*.*	Akira and Fog ransomware
Veeam Backup and Replication Deserialization Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINKS
	CWE-502	T1059: Command and Scripting Interpreter; T1068 : Exploitation for Privilege Escalation	https://www.veeam.com/kb4600


CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
<u>CVE-2024-28987</u>		WHD 12.8.3 HF1 and all previous versions	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS	cpe:2.3:a:solarwinds:web_help_desk:12.8.3_hotfix_1:~.*.*.*.*.*.*.*	-
SolarWinds Web Help Desk Hardcoded Credential Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-798	T1190: Exploit Public-Facing Application T0891: Hardcoded Credentials	https://support.solarwinds.com/SuccessCenter/s/article/SolarWinds-Web-Help-Desk-12-8-3-Hotfix-2




CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2024-9680		Firefox Version Prior to 131.0.2, Firefox ESR Version Prior to 128.3.1, and Firefox ESR Version Prior to 115.16.1	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS	cpe:2.3:a:mozilla:firefox:*:*:*:*:*:*	
Mozilla Firefox Use-After-Free Vulnerability		cpe:2.3:a:mozilla:firefox_esr:*:*:*:*:*:*	-
	CWE ID	ASSOCIATED TTPs	PATCH LINKS
	CWE-416	T1059: Command and Scripting Interpreter; T1189: Drive-by Compromise	https://www.mozilla.org/en-US/firefox/enterprise/#download




CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2024-30088		Windows Kernel	APT34
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS	cpe:2.3:o:microsoft:windows:*:*:*:*:*:*	
Microsoft Windows Kernel TOCTOU Race Condition Vulnerability		cpe:2.3:o:microsoft:windows_server:*:*:*:*:*:*	StealHook, DULLDROP
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-367	T1068: Exploitation for Privilege Escalation	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-30088



CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2024-9380		Ivanti CSA (Cloud Services Appliance) Version 5.0.1 and prior	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS	cpe:2.3:a:ivanti:endpoint_manager_cloud_services_appliance:4.6:-:*:*:*:*:*	-
Ivanti Cloud Services Appliance (CSA) OS Command Injection Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINKS
	CWE-77	T1059: Command and Scripting Interpreter, T1190 : Exploit Public-Facing Application, T1078 : Valid Accounts	https://forums.ivanti.com/s/article/Ivanti-Cloud-Services-Application-5-0-2-Download-Release-Notes-Patch-History

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2024-9379		Ivanti CSA (Cloud Services Appliance) Version 5.0.1 and prior	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS	cpe:2.3:a:ivanti:endpoint_manager_cloud_services_appliance:4.6:-:*:*:*:*:*	-
Ivanti Cloud Services Appliance (CSA) SQL Injection Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-89	T1078 : Valid Accounts, T1190 : Exploit Public-Facing Application	https://forums.ivanti.com/s/article/Ivanti-Cloud-Services-Application-5-0-2-Download-Release-Notes-Patch-History

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2024-23113		Fortinet FortiOS versions 7.4.0 through 7.4.2, 7.2.0 through 7.2.6, 7.0.0 through 7.0.13, FortiProxy versions 7.4.0 through 7.4.2, 7.2.0 through 7.2.8, 7.0.0 through 7.0.14, FortiPAM versions 1.2.0, 1.1.0 through 1.1.2, 1.0.0 through 1.0.3, FortiSwitchManager versions 7.2.0 through 7.2.3, 7.0.0 through 7.0.3	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOM WARE
NAME	BAS ATTACKS		
Fortinet Multiple Products Format String Vulnerability		cpe:2.3:a:fortinet:fortiproxy:*:*:*:*:*:*:* cpe:2.3:a:fortinet:fortiswitchmanager:*:*:*:*:*:*:*	-
	CWE ID	ASSOCIATED TTPs	PATCH LINKS
	CWE-314	T1059: Command and Scripting Interpreter; T1068: Exploitation for Privilege Escalation	https://www.fortiguard.com/psirt/FG-IR-24-029

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
<u>CVE-2024-43573</u>		Windows: 10 - 11 23H2 Windows Server: 2016 – 2022 23H2	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOM WARE
NAME	BAS ATTACKS		
Windows MSHTML Platform Spoofing Vulnerability		cpe:2.3:o:microsoft:windows:*:*:*:*:*:* cpe:2.3:o:microsoft:windows_server:*:*:*:*:*:*	-
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-79	T1059: Command and Scripting Interpreter, T1204 : User Execution, T1189 : Drive-by Compromise	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-43573

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
<u>CVE-2024-43572</u>		Windows: 10 - 11 23H2 Windows Server: 2008 – 2022 23H2	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS	cpe:2.3:o:microsoft:windows:*:*:*:*:*:* cpe:2.3:o:microsoft:windows_server:*:*:*:*:*:* *	
Microsoft Management Console Remote Code Execution Vulnerability			-
	CWE ID	ASSOCIATED TTPs	PATCH LINKS
	CWE-707	T1059: Command and Scripting Interpreter, T1204 : User Execution, T1204.002: Malicious File	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-43572

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2024-43047	 ZERO-DAY	FastConnect 6700, FastConnect 6800, FastConnect 6900, FastConnect 7800, QAM8295P, QCA6174A, QCA6391, QCA6426, QCA6436, QCA6574AU, QCA6584AU, QCA6595, QCA6595AU, QCA6688AQ, QCA6696, QCA6698AQ, QCS410, QCS610, QCS6490, Qualcomm® Video Collaboration VC1 Platform, Qualcomm® Video Collaboration VC3 Platform, SA4150P, SA4155P, SA6145P, SA6150P, SA6155P, SA8145P, SA8150P, SA8155P, SA8195P, SA8295P, SD660, SD865 5G, SG4150P, Snapdragon 660 Mobile Platform, Snapdragon 680 4G Mobile Platform, Snapdragon 685 4G Mobile Platform (SM6225-AD), Snapdragon 8 Gen 1 Mobile Platform, Snapdragon 865 5G Mobile Platform, Snapdragon 865+ 5G Mobile Platform (SM8250-AB), Snapdragon 870 5G Mobile Platform (SM8250-AC), Snapdragon 888 5G Mobile Platform, Snapdragon 888+ 5G Mobile Platform (SM8350-AC), Snapdragon Auto 5G Modem-RF, Snapdragon Auto 5G Modem-RF Gen 2, Snapdragon X55 5G Modem-RF System, Snapdragon XR2 5G Platform, SW5100, SW5100P, SXR2130, WCD9335, WCD9341, WCD9370, WCD9375, WCD9380, WCD9385, WCN3950, WCN3980, WCN3988, WCN3990, WSA8810, WSA8815, WSA8830, WSA8835	-
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS	cpe:2.3:o:qualcomm:fastconnect_firmware:-:*:*:*:*:*:* cpe:2.3:o:qualcomm:snapdragon_auto:-:*:*:*:*:*:* cpe:2.3:o:qualcomm:snapdragon_compute:-:*:*:*:*:*:* cpe:2.3:o:qualcomm:snapdragon_connectivity:-:*:*:*:*:*:* cpe:2.3:o:qualcomm:snapdragon_consumerIoT:-:*:*:*:*:*:* cpe:2.3:o:qualcomm:snapdragon_industrialIoT:-:*:*:*:*:*:* cpe:2.3:o:qualcomm:snapdragon_mobile:-:*:*:*:*:*:* cpe:2.3:o:qualcomm:snapdragon_wearables:-:*:*:*:*:*:*	-
Qualcomm Multiple Chipsets Use-After-Free Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
CWE-416	T1059: Command and Scripting Interpreter; T1495 : Firmware Corruption	https://docs.qualcomm.com/product/publicresources/securitybulletin/october-2024-bulletin.html	

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
<u>CVE-2024-45519</u>		Zimbra Collaboration (ZCS) before 8.8.15 Patch 46, 9 before 9.0.0 Patch 41, 10 before 10.0.9, and 10.1 before 10.1.1	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS	cpe:2.3:a:zimbra:collabo	
Synacor Zimbra Collaboration Command Execution Vulnerability		ration:*:*:*:*:*:*	-
	CWE ID	ASSOCIATED TTPs	PATCH LINKS
	CWE-863 CWE-284	T1059: Command and Scripting Interpreter T1190: Exploit Public-Facing Application	https://wiki.zimbra.com/wiki/Zimbra_Releases/8.8.15/P46 ; https://wiki.zimbra.com/wiki/Zimbra_Releases/9.0.0/P41 ; https://wiki.zimbra.com/wiki/Zimbra_Releases/10.0.9 ; https://wiki.zimbra.com/wiki/Zimbra_Releases/10.1.1

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
<u>CVE-2024-29824</u>		Ivanti Endpoint Manager 2022 SU5 and prior versions	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	BAS ATTACKS	cpe:2.3:a:ivanti:endpoint_	
Ivanti Endpoint Manager (EPM) SQL Injection Vulnerability		manager:*:*:*:*:*:*	-
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-89	T1059: Command and Scripting, T1562.010: Downgrade Attack	https://forums.ivanti.com/s/article/KB-Security-Advisory-EPM-May-2024

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.

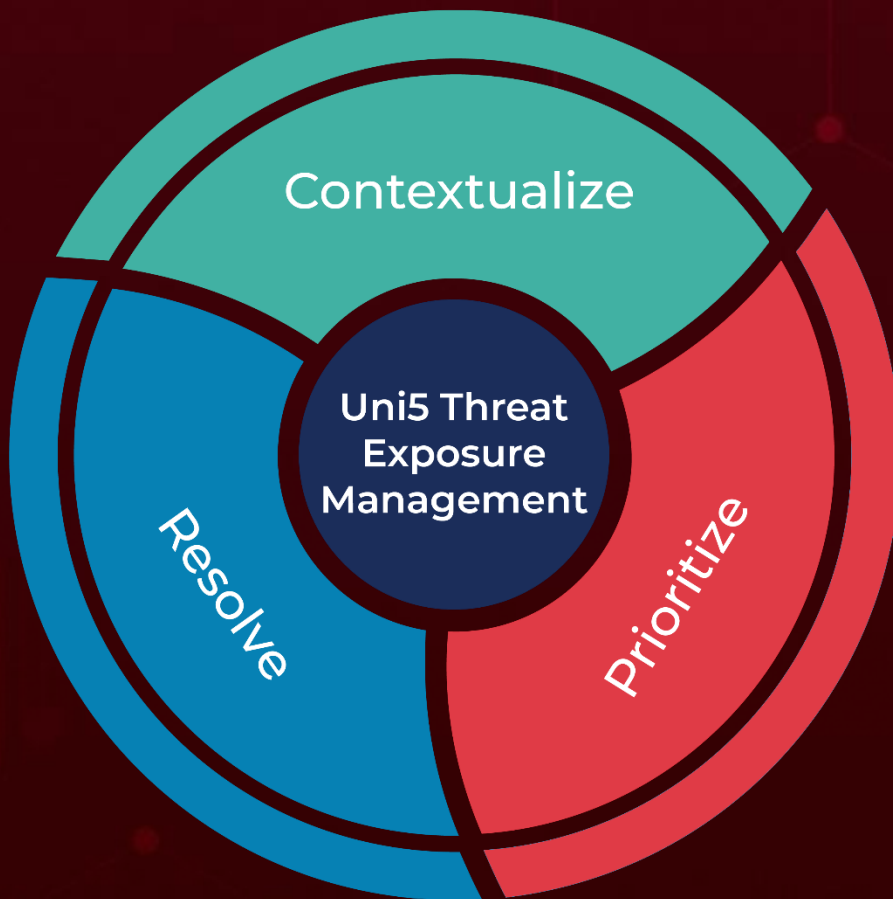
BAS Attacks: “BAS attacks” are the simulated cyber-attacks that can be carried out by our in-house Uni5's Breach and Attack Simulation (BAS), which organizations could use to identify vulnerabilities and improve their overall security posture.

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

November 11, 2024 • 9:00 PM

© 2024 All Rights are Reserved by Hive Pro



More at www.hivepro.com