Date of Publication

February 23, 2023

Hive Pro

Hiveforce Labs

CISA KNOWN EXPLOITED VULNERABILITY CATALOG

January 2023

CVEs

CVE	Affected Product	BAS Attacks	PATCH	Due Date
CVE-2017-11357	Telerik User Interface (UI) for ASP.NET AJAX	✓	✓	February 16, 2023
CVE-2022-47966	Zoho ManageEngine	✓	✓	February 13, 2023
CVE-2022-44877	Control Web Panel	✓	✓	February 7, 2023
CVE-2022-41080	Microsoft Exchange Server	✓	✓	January 31, 2023
CVE-2023-21674	Microsoft Windows	✓	✓	January 31, 2023

Vulnerability Details

CVE	NAME	Affected Product	Affected CPE
CVE-2017-11357	Telerik UI for ASP.NET AJAX Insecure Direct Object Reference Vulnerability	UI for ASP.NET AJAX: 2016.3.1027 - 2017.2.621	cpe:2.3:a:progress:ui_for_aspnet_ajax:*:*:*:*:*:*:*:*
	Associated Actor	**CWE ID**	**Patch Link**
	Unknown Chinese Threat Actor	CWE-20	https://docs.telerik.com/devtools/aspnet-ajax/knowledge-base/asyncupload-insecure-direct-object-reference
	Associated Named Attack		

CVE	NAME	Affected Product	Affected CPE
CVE-2022-47966	Zoho ManageEngine Multiple Products Remote Code Execution Vulnerability	ManageEngine Access Manager Plus: 4.1 4100 - 4.3 4307, Vulnerability Manager Plus: before 10.1.2220.18, Remote Monitoring and Management (RMM): before 10.1.41, Zoho ManageEngine Remote Access Plus: before 10.1.2228.11, Patch Manager Plus: before 10.1.2220.18, Password Manager Pro: before 12124, PAM 360: before 5713, OS Deployer: before 1.1.2243.1, Key Manager Plus: before 6401, Endpoint DLP: before 10.1.2137.6, Endpoint Central MSP: before 10.1.2228.11, Endpoint Central: before 10.1.2228.11, Device Control Plus: before 10.1.2220.18, ManageEngine Browser Security Plus: before 11.1.2238.6, ManageEngine Application Control Plus: before 10.1.2220.18, ManageEngine Analytics Plus: before 5150, Zoho ManageEngine ADManager Plus: before 7162, Zoho ManageEngine Active Directory 360: before 4310, ManageEngine AssetExplorer: before 6983, Zoho ManageEngine ServiceDesk Plus MSP: before 13001, Zoho ManageEngine SupportCenter Plus: before 11026, Zoho ManageEngine ADAudit Plus: before 7081, Zoho ManageEngine ADSelfService Plus: before 6211, Zoho ManageEngine ServiceDesk Plus: before 14.0 14004	cpe:2.3:a:zohocorp:manageengine_access_manager_plus:*:*:*:*:*:*:*:* cpe:2.3:a:zohocorp:manageengine_ad360:*:*:*:*:*:*:*:* cpe:2.3:a:zohocorp:manageengine_adaudit_plus:*:*:*:*:*:*:*:* cpe:2.3:a:zohocorp:manageengine_admanager_plus:*:*:*:*:*:*:*:* cpe:2.3:a:zohocorp:manageengine_adselfservice_plus:*:*:*:*:*:*:*:* cpe:2.3:a:zohocorp:manageengine_analytics_plus:*:*:*:*:*:*:*:* cpe:2.3:a:zohocorp:manageengine_assetexplorer:*:*:*:*:*:*:*:* cpe:2.3:a:zohocorp:manageengine_key_manager_plus:*:*:*:*:*:*:*:* cpe:2.3:a:zohocorp:manageengine_pam360:*:*:*:*:*:*:*:* cpe:2.3:a:zohocorp:manageengine_password_manager_pro:*:*:*:*:*:*:*:* cpe:2.3:a:zohocorp:manageengine_servicedesk_plus:*:*:*:*:*:*:*:* cpe:2.3:a:zohocorp:manageengine_servicedesk_plus_msp:*:*:*:*:*:*:*:* cpe:2.3:a:zohocorp:manageengine_supportcenter_plus:*:*:*:*:*:*:*:* cpe:2.3:a:zohocorp:application_control_plus:*:*:*:*:*:*:*:* cpe:2.3:a:zohocorp:manageengine_browser_security_plus:*:*:*:*:*:*:*:* cpe:2.3:a:zohocorp:manageengine_desktop_central:*:*:*:*:-:*:*:* cpe:2.3:a:zohocorp:manageengine_desktop_central:*:*:*:*:managed_service_providers:*:*:* cpe:2.3:a:zohocorp:manageengine_device_control_plus:*:*:*:*:*:*:*:* cpe:2.3:a:zohocorp:manageengine_endpoint_dlp_plus:*:*:*:*:*:*:*:* cpe:2.3:a:zohocorp:manageengine_os_deployer:*:*:*:*:*:*:*:* cpe:2.3:a:zohocorp:manageengine_patch_manager_plus:*:*:*:*:*:*:*:* cpe:2.3:a:zohocorp:manageengine_remote_access_plus:*:*:*:*:*:*:*:* cpe:2.3:a:zohocorp:manageengine_rmm_central:*:*:*:*:*:*:*:* cpe:2.3:a:zohocorp:manageengine_vulnerability_manager_plus:*:*:*:*:*:*:*:*
	Associated Actor	**CWE ID**	**Patch Link**
	Unknown	CWE-20	https://www.manageengine.com/security/advisory/CVE/cve-2022-47966.html
	Associated Named Attack		

CVE	NAME	Affected Product	Affected CPE
CVE-2022-44877	CWP Control Web Panel OS Command Injection Vulnerability	CWP Panel: 0.9.8.1051 - 0.9.8.1146	cpe:2.3:a:cwp_-_control_web_panel:cwp_panel:*:*:*:*:*:*:*:*
	Associated Actor	**CWE ID**	**Patch Link**
	Unknown	CWE-78 / CWE-74 / CWE-707	https://control-webpanel.com/changelog#1669855527714-450fb335-6194
	Associated Named Attack		

CVE	NAME	Affected Product	Affected CPE
CVE-2022-41080	Microsoft Exchange Server Privilege Escalation Vulnerability	Microsoft Exchange Server 2016 Cumulative Update 22, Microsoft Exchange Server 2019 Cumulative Update 11, Microsoft Exchange Server 2013 Cumulative Update 23, Microsoft Exchange Server 2019 Cumulative Update 12, Microsoft Exchange Server 2016 Cumulative Update 23	cpe:2.3:a:microsoft:exchange_server:2013:cumulative_update_23:*:*:*:*:*:*:*, cpe:2.3:a:microsoft:exchange_server:2016:cumulative_update_22:*:*:*:*:*:*:*, cpe:2.3:a:microsoft:exchange_server:2016:cumulative_update_23:*:*:*:*:*:*:*, cpe:2.3:a:microsoft:exchange_server:2019:cumulative_update_11:*:*:*:*:*:*:*, cpe:2.3:a:microsoft:exchange_server:2019:cumulative_update_12:*:*:*:*:*:*:*
	Associated Actor	**CWE ID**	**Patch Link**
	Unknown	CWE-264	https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2022-41080
	Associated Named Attack		
	SilverArrow backdoor		

CVE	NAME	Affected Product	Affected CPE
CVE-2023-21674*	Microsoft Windows Advanced Local Procedure Call (ALPC) Privilege Escalation Vulnerability	Windows: 8.1 - 11 22H2 Windows Server: 2012 R2 - 2022 20H2	cpe:2.3:o:microsoft:windows:*:*:*:*:*:*:*:*
	Associated Actor	**CWE ID**	**Patch Link**
	Unknown	CWE-119	https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2023-21674
	Associated Named Attack		

* zero-day vulnerability

Recommendations

- Adhere to BINDING OPERATIONAL DIRECTIVE 22-01 provided by CISA.
- Follow the patch links provided to update vulnerable assets.
- If the affected product cannot be updated or is no longer supported, remove it from the organization's networks.

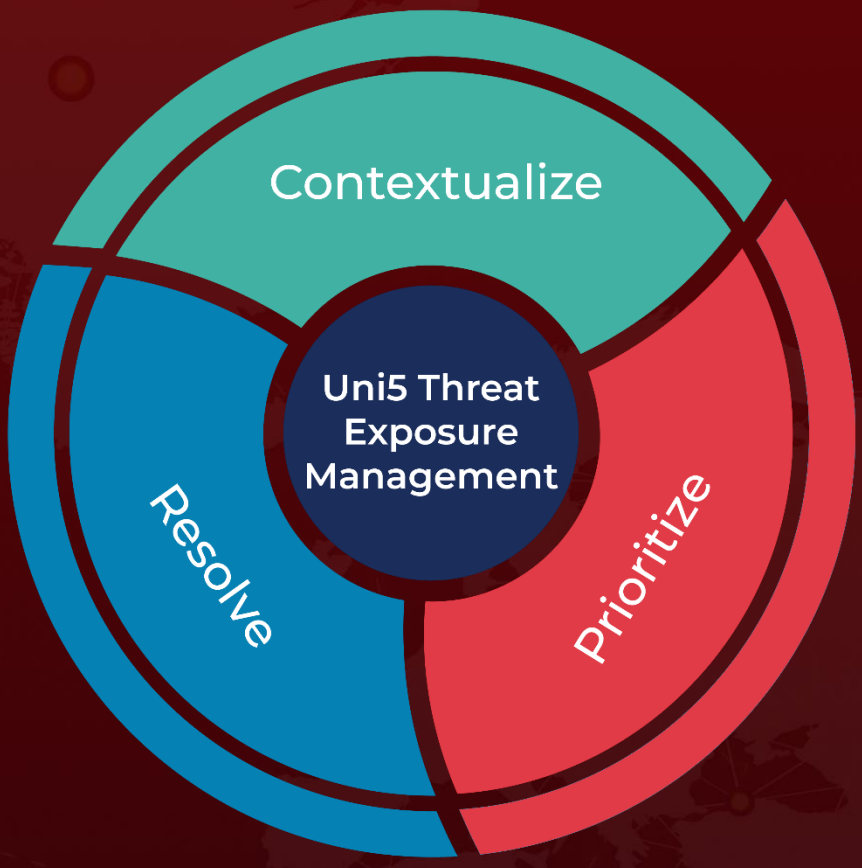
References

https://www.cisa.gov/known-exploited-vulnerabilities-catalog

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 23, 2023 . 5:00 AM

More at www.hivepro.com