Hive Pro®

Threat Level

Red

Hiveforce Labs

THREAT ADVISORY

VULNERABILITY REPORT

Admins Urged to Uninstall VMware EAP Amid Critical Flaws

Date of Publication	Admiralty Code	TA Number
February 21, 2024	A1	TA2024067

Summary

First Seen: February 20, 2024
Affected Products: VMware Enhanced Authentication Plug-in (EAP)
Impact: VMware has issued a warning to administrators regarding two unaddressed security vulnerabilities necessitating the removal of an outdated authentication plugin. Identified as CVE-2024-22245 and CVE-2024-22250, these vulnerabilities enable session hijacking and authentication relay attacks targeting the VMware Enhanced Authentication Plug-in (EAP) within Windows domain environments.

CVEs

CVE	NAME	AFFECTED PRODUCT	ZERO -DAY	CISA KEV	PATCH
CVE-2024-22245	VMware Arbitrary Authentication Relay Vulnerability	VMware Enhanced Authentication Plug-in (EAP)	⊗	⊗	⊗
CVE-2024-22250	VMware Session Hijack Vulnerability	VMware Enhanced Authentication Plug-in (EAP)	⊗	⊗	⊗

Vulnerability Details

#1

VMware has issued a warning to administrators about two unpatched security vulnerabilities that necessitate the removal of an outdated authentication plugin. These vulnerabilities, identified as CVE-2024-22245 and CVE-2024-22250, open the door to session hijacking and authentication relay attacks against the VMware EAP in Windows domain environments. EAP enables smooth login to vSphere administrative interfaces; Admins must install the EAP manually as it does not come with default installation.

#2 CVE-2024-22245 is a vulnerability related to Arbitrary Authentication Relay in the VMware Enhanced Authentication Plug-in (EAP). By installing EAP on their web browser, a remote attacker can deceive a target domain user into requesting and forwarding service tickets for random Active Directory Service Principal Names (SPNs).

#3 The vulnerability CVE-2024-22250, identified in the VMware Enhanced Authentication Plug-in (EAP), allows for session hijacking. This vulnerability stems from the method in which EAP initiates and oversees Active Directory (AD) sessions. Specifically, it enables a local user to seize control of a privileged EAP session on the same system.

#4 VMware announced the deprecation of EAP in March 2021. Administrators must uninstall the outdated Plug-in Windows service and the in-browser plugin/client in order to address security vulnerabilities. The Windows service can be disabled or uninstalled using **PowerShell instructions**.

Vulnerabilities

CVE ID	AFFECTED PRODUCTS	AFFECTED CPE	CWE ID
CVE-2024-22245	Enhanced Authentication Plug-in (EAP): All versions	cpe:2.3:a:vmware:EnhancedAuthenticationPlug-in:*:*:*:*:*:*:*	CWE-287
CVE-2024-22250	Enhanced Authentication Plug-in (EAP): All versions	cpe:2.3:a:vmware:EnhancedAuthenticationPlug-in:*:*:*:*:*:*:*	CWE-384

Recommendations

Remove VMware EAP: Administrators must uninstall the VMware Enhanced Authentication Plug-in in-browser plugin/client and the VMware Plug-in Service Windows service in order to fix the security vulnerabilities CVE-2024-22245 and CVE-2024-22250.

Least Privilege: Adhere to the idea of "least privilege" by giving users/ application only the essential permissions they need for their tasks. This strategy reduces the effects of vulnerabilities related to privilege escalation.

Potential MITRE ATT&CK TTPs

TA0042 Resource Development	TA0001 Initial Access	TA0004 Privilege Escalation	TA0006 Credential Access
TA0009 Collection	T1588 Obtain Capabilities	T1588.006 Vulnerabilities	T1068 Exploitation for Privilege Escalation
T1558 Steal or Forge Kerberos Tickets	T1566 Phishing	T1566.001 Spearphishing Attachment	T1185 Browser Session Hijacking

Patch Details

Since the plugin is no longer supported and there are no forthcoming security updates, it is strongly advised to uninstall it from your systems following the provided instructions.

Link:
https://kb.vmware.com/s/article/96442

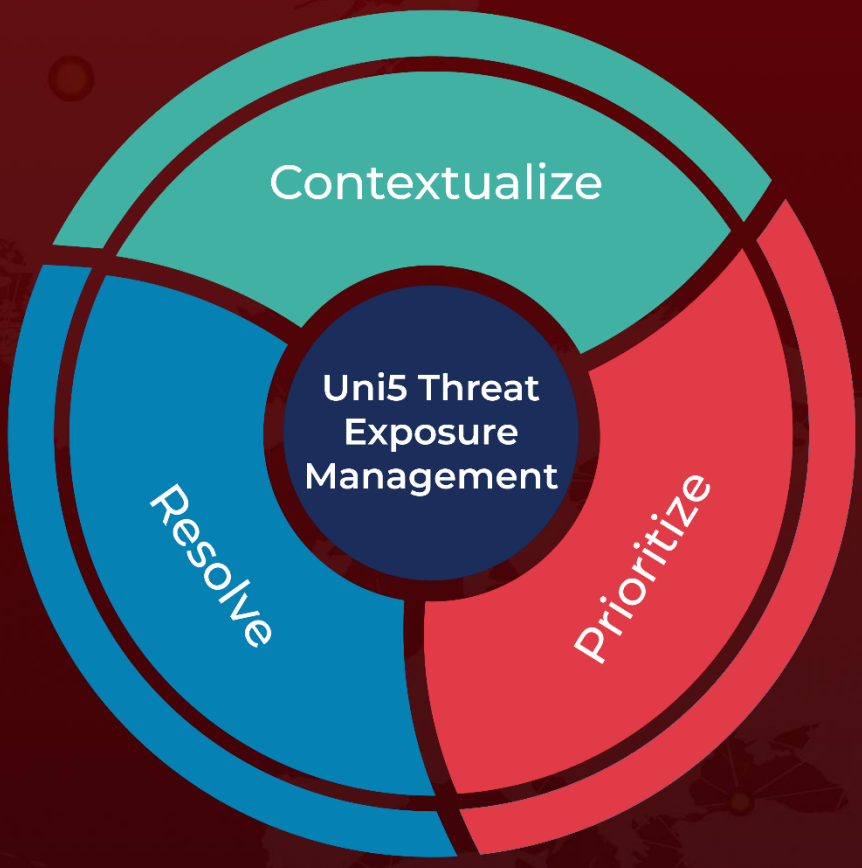
References

https://www.vmware.com/security/advisories/VMSA-2024-0003.html

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 21, 2024 • 5:40 AM

More at www.hivepro.com