AL2024_03 Critical Security Flaw Found in Deprecated VMware EAP Plugin: Uninstall Now! (March 21st, 2024)

Description

A critical security vulnerability (CVE-2024-22245) has been discovered in the VMware Enhanced Authentication Plugin (EAP), a tool allowing direct login to vSphere management interfaces. This vulnerability exposes users to potential account takeover and data breaches.

Details

A critical security vulnerability, dubbed CVE-2024-22245, has been identified in the Enhanced Authentication Plugin (EAP), a tool designed for convenient login to vSphere management interfaces. This vulnerability, classified as an "arbitrary authentication relay," throws open the doors for attackers to potentially hijack accounts and wreak havoc on your systems.

When a user with EAP installed clicks on it, their system unknowingly requests and relays service tickets i.e. digital keys, for any desired account within Active Directory. This grants the attacker unauthorized access to sensitive data and functionalities.

To make matters worse, another vulnerability (CVE-2024-22250) lurks within EAP. This "session hijacking" vulnerability allows attackers with local access to a Windows system to seize control of a privileged EAP session, potentially escalating their access even further.

Fortunately, not everyone using vSphere is in danger. This vulnerability only impacts users who have manually installed EAP on their Windows systems, specifically for accessing vSphere through the vSphere Client. If you have not done this, you are safe. Since patching is not an option, immediate action is crucial. The only way to mitigate the risk is to completely uninstall the EAP plugin from all affected Windows systems. Do not delay, as even a single vulnerable system can be a gateway for attackers to compromise your entire environment.

Remediation

Immediate action required: Uninstall the VMware EAP plugin from all affected Windows systems.

- Alternative Authentication Methods: Use supported and secure methods like vSphere Client certificates or Active Directory integration for vSphere management.
- No Patch Available: VMware will not patch these vulnerabilities due to EAP being deprecated.

Additional Notes

- This vulnerability only impacts users who have manually installed EAP on Windows systems for vSphere access.
- The disclosed Joomla! XSS vulnerabilities (CVE-2024-21726) are addressed in versions 5.0.3 and 4.4.3.

The Guyana National CIRT recommends that users and administrators review this alert and apply it where necessary.

References

- The Hacker News. (21st February 2024). *VMware Alert: Uninstall EAP now - Critical flaw puts active directory at risk*. Retrieved from The Hacker News. https://thehackernews.com/2024/02/vmware-alert-uninstall-eap-now-critical.html
- Gatlan, S. (20th, February 2024). VMware urges admins to remove deprecated, vulnerable auth plug-in. Retrieved from *BleepingComputer*. https://www.bleepingcomputer.com/news/security/vmware-urges-admins-to-remove-deprecated-vulnerable-auth-plug-in/