February 20, 2024

Overall rating: Critical

This is a technical bulletin intended for technical audiences.

Summary

The Vulnerability and Risk Management (VRM) Team has been made aware VMware released a security advisory to address vulnerabilities in the following product:

- VMware Enhanced Authentication Plug-in (EAP)

Technical Details

The VMware Enhanced Authentication Plug-in (EAP) contains an Arbitrary Authentication Relay vulnerability. VMware has evaluated the severity of this issue to be in the Critical severity range with a maximum CVSSv3 base score of 9.6.

Known Attack Vectors

A malicious actor could trick a target domain user with EAP installed in their web browser into requesting and relaying service tickets for arbitrary Active Directory Service Principal Names (SPNs).

Exploitability Metrics
Attack Vector: Network
Attack Complexity: Low
Privileges Required: None
User Interaction: None

This vulnerability is rated as a **CRITICAL** risk. A software update exists to address these risks.

Action Required

- Locate the device or application and investigate.
- Notify business owner(s).
- Perform mitigating actions, as required.

Please notify VRM with any questions or concerns you may have.

References

- CVE-2024-22245, CVE-2024-22250
- VMware Security Advisory - VMSA-2024-0003
- VMware Security Advisories