Overall rating: High

This is a technical bulletin intended for technical audiences.

Summary

The Vulnerability and Risk Management (VRM) Team has been made aware of a vulnerability in the installer script of Cisco AppDynamics PHP Agent. The vulnerability affects Cisco AppDynamics PHP Agent.

Technical Details

A vulnerability in the installer script of Cisco AppDynamics PHP Agent could allow an authenticated, local attacker to elevate privileges on an affected device.

This vulnerability is due to insufficient permissions that are set by the PHP Agent Installer on the PHP Agent install directory. An attacker could exploit this vulnerability by modifying objects in the PHP Agent install directory, which would run with the same privileges as PHP. A successful exploit could allow a lower-privileged attacker to elevate their privileges to root on an affected device.

> **Exploitability Metrics**
> Attack Vector: Local
> Attack Complexity: Low
> Privileges Required: None
> User Interaction: None

This vulnerability is rated as a **HIGH** risk. A software update exists to address this risk.

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-2023-20274
- Cisco AppDynamics PHP Agent Privilege Escalation Vulnerability
- VRM Vulnerability Reports