April 5, 2024

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 VMware vulnerabilities. The vulnerability affects VMware SD-WAN (Edge) prior to 4.5.1+ and 5.0.1+ and VMware SD-WAN (Orchestrator) prior to 5.0.1+.

Technical Details

VMware SD-WAN Edge contains an unauthenticated command injection vulnerability potentially leading to remote code execution. VMware has evaluated the severity of this issue to be in the Important severity range with a maximum CVSSv3 base score of 7.4. A malicious actor with local access to the Edge Router UI during activation may be able to perform a command injection attack that could lead to full control of the router.

VMware SD-WAN Orchestrator contains an open redirect vulnerability. VMware has evaluated the severity of this issue to be in the Important severity range with a maximum CVSSv3 base score of 7.1. A malicious actor may be able to redirect a victim to an attacker-controlled domain due to improper path handling leading to sensitive information disclosure.

Exploitability Metrics
Attack Vector: Local
Attack Complexity: High
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-2024-22246, CVE-2024-22247, CVE-2024-22248
- VMSA-2024-0008
- VRM Vulnerability Reports