Cisco Secure Network Analytics Manager Privilege Escalation Vulnerability

Overview

A medium-severity privilege escalation vulnerability was found in Cisco's Secure Network Analytics Manager and Virtual Manager. The flaw, tracked as CVE-2025-20256 (CVSS 6.5), is caused by insufficient input validation in the web management interface. An attacker with valid admin credentials can craft malicious input to execute commands with root privileges on the underlying operating system.

TL;DR

Cisco has patched a vulnerability (CVE-2025-20256) that allows administrators of Secure Network Analytics Manager to execute arbitrary commands as root.

While exploitation requires valid admin credentials, the impact is significant - command execution at the OS level. No workarounds exist, and all affected systems should be updated immediately.

CVE-2025-20256 allows an attacker with existing admin access to bypass input restrictions and run arbitrary commands directly on the operating system as the root user. The core issue lies in how the web interface handles certain inputs, failing to properly sanitize them before execution. While privilege is required to exploit it, the ability to escalate from admin to root significantly increases the potential damage, especially in environments where Secure Network Analytics plays a central monitoring role.

If an attacker gains access to an admin account they could take full control of the host device. Aspire recommends patching as soon as possible.

Aspire Protects

- **Patch –** Patch all affected Cisco Secure Network Analytics Managers using the fixed rollup versions.
- Audit access logs for suspicious or unexpected administrative activity.
- Consider enhanced monitoring on SNA infrastructure to catch misuse or command-level anomalies.
- Review internal segmentation to ensure SNAs are not accessible from broad internal ranges.

TTPs to Watch

Privilege Escalation

- Exploitation for Privilege Escalation [T1068] - A compromised admin account can abuse this vulnerability to escalate to root.

Execution

- Command and Scripting Interpreter [T1059] – Exploitation results in direct OS-level command execution.

Persistence

- Valid Accounts [T1078] – An attacker may use stolen or misused admin credentials to trigger this flaw without triggering external alerts.

IoCs

There are no known IoCs associated with the above vulnerability at this time. Aspire is actively monitoring and will notify customers if any are found. For more details on how we can help protect your organization, contact Aspire's Customer Success Management team.

Targeted Industries

This vulnerability affects any organization using Cisco Secure Network Analytics, especially in industries where privileged access is tightly monitored:

- Healthcare
- Public Sector
- Energy and Utilities
- Finance
- Legal and Professional Services

Aspire Service Offerings

- **Aspire Managed XDR (MXDR)**
  - Aspire Managed XDR (MXDR) combines next-generation eXtended Detection and Response (XDR) technology, a 24x7 security operations center (SOC), and the expertise of a US-based team of security

professionals to identify and respond to threats across a broader attack surface.
    - Building on the existing capabilities of Managed Detection and Response (MDR), Aspire Managed XDR integrates and correlates telemetry from endpoints, network, cloud, email, identity, and more. This advanced platform creates valuable context enabling end-to-end visibility across all threat vectors.
    - Experienced security analysts and incident responders deliver 24x7 threat detection, analysis, and investigations – with both automated and human-led response actions to quickly mitigate cyber attacks.
- **Aspire Incident Response**
    - The ability to respond effectively to data breaches is critical to every organization. When attacks occur, IT leaders need a process that will ultimately maintain business continuity, protect the company reputation, and avoid fines, legal fees, and remediation costs.
    - Aspire offers incident response services to help you prepare for, manage, and recover from data breaches and network attacks. An experienced team uses industry-leading threat intelligence and the most current security technology to quickly respond to attacks, reduce damage, and minimize exposure.

Supporting Documentation

Cisco Secure Network Analytics Manager Privilege Escalation Vulnerability

NVD - CVE-2025-20256