Cisco Secure Network Analytics Privilege Escalation Vulnerability

Overview

Cisco released a security advisory addressing a high-severity vulnerability (CVE-2025-20178, CVSS 6) in Secure Network Analytics (SNA). The flaw could allow an authenticated user to escalate their privileges to administrative level on affected systems.

Affected Products

- Secure Network Analytics Data Store & Virtual Data Store
- Flow Collector & Virtual Flow Collector
- Flow Sensor & Virtual Flow Sensor
- Manager & Virtual Manager
- UDP Director & Virtual UDP Director

The issue stems from insufficient integrity checks in device backup files. An attacker with admin access could craft a malicious backup file and restore it to a vulnerable SNA system. If successful, they could gain shell access with root privileges. This affects both physical and virtual deployments of the impacted products.

This is a reminder that even backup functionality can be abused when basic integrity checks are missing. If an attacker already has admin credentials, whether from insider threats or credential theft, this vulnerability gives them an easy path to root-level system control. This vulnerability has not been exploited in the wild and there are no workarounds. Patch immediately if you are running Secure Network Analytics version 7.5x.

Aspire Protects

- **Patch –** Please upgrade to the following fixed versions:
  - 7.5.0 ROLLUP20250218-01
  - 7.5.1 ROLLUP20250218-01
  - 7.5.2 ROLLUP20250319-01
- Monitor systems for shell activity on affected appliances.
- Review current admin accounts and verify that no unauthorized backup restores have occurred.

TTPs to Watch

Privilege Escalation

- Valid Accounts [T1078] – The attacker may have used legitimate admin credentials to log in.

Execution

- Command and Scripting Interpreter [T1059] – The attacker may have gained shell access through backup file injection.

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

Organizations across several sectors may be impacted due to widespread use of Secure Network Analytics for network monitoring and traffic visibility.

- Healthcare
- Education
- Retail
- Finance
- Manufacturing
- Government
- Energy

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 Privilege Escalation Vulnerability

NVD - CVE-2025-20178