Cisco Addresses Finesse and Catalyst SD-WAN Manager Vulnerabilities

***Author**: Portia S. Cole – CTI Researcher*

TL;DR

Cisco patched two medium-severity vulnerabilities: CVE-2026-20175 affecting Cisco Finesse and CVE-2026-20262 affecting Cisco Catalyst SD-WAN Manager.

Successful exploitation could allow browser-based attacks or arbitrary file writes that may lead to root privilege escalation. Cisco has confirmed limited exploitation of the Cisco Catalyst SD-WAN Manager vulnerability.

Overview

Cisco addressed two medium-severity vulnerabilities affecting Cisco Finesse, a browser-based application used to manage contact center operations, and Cisco Catalyst SD-WAN Manager, a centralized platform used to configure and manage software-defined wide area networks (SD-WAN).

The vulnerabilities include:

- **CVE-2026-20175 (CVSS 6.1) – Cisco Finesse**
    - An insufficient input validation vulnerability that could allow an unauthenticated attacker to persuade a user to open a crafted link, resulting in arbitrary JavaScript execution within the user's browser session or access to sensitive information through the Cisco Finesse interface.
- **CVE-2026-20262 (CVSS 6.5) – Cisco Catalyst SD-WAN Manager**
    - An improper input validation vulnerability that could allow an authenticated attacker with write privileges to create or overwrite files on the underlying operating system through the web interface. The vulnerability may be leveraged to obtain root privileges. Cisco has confirmed limited exploitation.

Cisco has provided software updates to address both vulnerabilities. No workarounds are available.

Aspire Protects

- CVE-2026-20175 – Cisco Finesse
    - Upgrade Cisco Finesse to a fixed software release.

    - Remind users to avoid clicking unsolicited or unexpected links that reference Cisco Finesse.
- CVE-2026-20262 – Cisco Catalyst SD-WAN Manager
    - Upgrade Cisco Catalyst SD-WAN Manager to the latest fixed software release.
    - Review vmanage-server.log, vmanage-appserver.log, and serviceproxy-access.log for suspicious WAR file uploads or deployments.
    - Investigate unauthorized file creation or unexpected deployments if suspicious activity is identified.

TTPs to Watch

CVE-2026-20175 – Cisco Finesse Remote File Inclusion

Initial Access
- Drive-by Compromise [T1189] – The attacker may persuade a user to visit a crafted URL that loads malicious content into an active Cisco Finesse session.

Execution
- JavaScript [T1059.007] – The attacker may execute arbitrary JavaScript within the user's browser session.

Collection
- Data from Information Repositories [T1213] – The attacker may access sensitive information exposed through the affected interface.

CVE-2026-20262 – Cisco Catalyst SD-WAN Manager Arbitrary File Write

Initial Access
- Exploit Public-Facing Application [T1190] – The attacker may exploit the vulnerable web interface to upload a malicious file.

Persistence
- Server Software Component: Web Shell [T1505.003] – The attacker may deploy a malicious WAR file to establish persistent access.

Privilege Escalation
- Exploitation for Privilege Escalation [T1068] – The attacker may leverage the arbitrary file write vulnerability to obtain root privileges.

IoCs

CVE-2026-20262

Log Artifacts

- vmanage-server.log
  - uploaded Remote Access Anyconnect profile file: ../../../../var/lib/wildfly/standalone/deployments/suspicious.war
- vmanage-appserver.log
  - WFLYSRV0010: Deployed "suspicious.war" (runtime-name: "suspicious.war")

serviceproxy-access.log

- POST /suspicious/index[.]jsp HTTP/1.1

File Names

- Suspicious.war

File Paths

- /var/lib/wildfly/standalone/deployments/suspicious.war

Affected Log Locations

- /var/log/nms/vmanage-server.log
- /var/log/nms/vmanage-appserver.log
- /var/log/nms/containers/service-proxy/serviceproxy-access.log

CVE-2026-20175 – Cisco Finesse

- No public indicators of compromise have been released by Cisco.

Targeted Industries

Organizations that use Cisco Finesse for contact center operations or Cisco Catalyst SD-WAN Manager to manage enterprise networks may be affected.

- Education
- Energy
- Finance
- Healthcare
- Legal
- Manufacturing
- Public Sector
- Retail

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 Finesse Remote File Inclusion Vulnerability

Cisco Catalyst SD-WAN Manager Arbitrary File Write Vulnerability