MULTIPLE VULNERABILITIES IN CISCO APIC

Vairav Advisory Report

Date: 2025-02-27

Vairav Cyber Threat Intelligence Team

Vairav Technology Security Pvt. Ltd.

Thirbam Sadak 148

Baluwatar, Kathmandu

Phone: +977 4541540

Mobile: +977-9820105900

Email: mail@vairavtech.com

EXECUTIVE SUMMARY

Multiple vulnerabilities, including CVE-2025-20116, CVE-2025-20117, CVE-2025-20118, and CVE-2025-20119, have been identified in Cisco's Application Policy Infrastructure Controller (APIC). The most severe of these vulnerabilities allows an authenticated, local attacker to overwrite critical system files, potentially causing a denial-of-service (DoS) condition, with a CVSS score of 6.0. If exploited, these vulnerabilities could lead to system instability, unauthorized command execution, sensitive information disclosure, and cross-site scripting (XSS) attacks.

VULNERABILITY DETAILS

CVE-2025-20116

- **Description:** A vulnerability in the web UI of Cisco APIC could allow an authenticated, remote attacker to perform a stored XSS attack. This issue arises from improper input validation, enabling an attacker to inject malicious code into specific web UI pages.
- **Impact:** Successful exploitation could allow the attacker to execute arbitrary script code within the web UI context or access sensitive browser-based information.
- **CVSS Score:** 4.8 (Medium)

CVE-2025-20117

- **Description:** A vulnerability in the CLI of Cisco APIC could allow an authenticated, local attacker to execute arbitrary commands as the root user on the underlying operating system. This vulnerability is due to insufficient validation of arguments passed to specific CLI commands.
- **Impact:** Exploitation could grant the attacker root-level command execution on the affected device.
- **CVSS Score:** 5.1 (Medium)

CVE-2025-20118

- **Description:** A vulnerability in the internal system processes of Cisco APIC could allow an authenticated, local attacker to access sensitive information. This issue is due to insufficient masking of sensitive information displayed through system CLI commands.

- **Impact:** An attacker could obtain sensitive information, which could be used to facilitate further attacks.
- **CVSS Score:** 4.4 (Medium)

CVE-2025-20119

- **Description:** A vulnerability in the system file permission handling of Cisco APIC could allow an authenticated, local attacker to overwrite critical system files, leading to a DoS condition. This vulnerability stems from a race condition in handling system files.
- **Impact:** Successful exploitation could render the device unstable or inoperative, causing a DoS condition.
- **CVSS Score:** 6.0 (Medium)

AFFECTED VERSIONS

Cisco APIC versions before:

- 6.0(8e)
- 6.1(2f)

EXPLOIT DETAILS

These vulnerabilities are particularly concerning in environments where Cisco APIC is used to manage network policies and configurations. Exploitation requires valid administrative credentials, limiting potential attackers to those with authorized access. However, once exploited, these vulnerabilities could lead to significant disruptions, including system outages, unauthorized access to sensitive information, and execution of arbitrary commands with elevated privileges.

RECOMMENDED ACTIONS

Patch & Upgrade: Cisco has released software updates to address these vulnerabilities. Administrators are advised to upgrade to the latest Cisco APIC versions:

- 6.0(8e)
- 6.1(2f)

ADDITIONAL SECURITY MEASURES

- **Access Control**: Restrict administrative access to the APIC system to trusted personnel only.
- **Monitoring**: Implement continuous monitoring to detect and respond to unusual activities promptly.
- **Input Validation**: Ensure proper input validation mechanisms are in place to prevent injection attacks.
- **Regular Audits**: Conduct regular security audits and vulnerability assessments to identify and mitigate potential risks.

REFERENCES

- https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-apic-multi-vulns-9ummtg5
- https://app.opencve.io/cve/CVE-2025-20116
- https://app.opencve.io/cve/CVE-2025-20117
- https://app.opencve.io/cve/CVE-2025-20118
- https://app.opencve.io/cve/CVE-2025-20119

CONTACT US

Vairav Technology Security Pvt. Ltd.

Cyber Defender from the land of Gurkha

Thirbam Sadak 148, Baluwatar

Kathmandu, Nepal

Phone: +977-01-4541540

Mobile: +977-9820105900

Email: sales@vairavtech.com

Website: https://vairavtech.com