GOVERNMENT OF THE REPUBLIC OF VANUATU

PRIME MINISTER'S OFFICE

CERTVU
DEPARTMENT OF COMMUNICATIONS & DIGITAL TRANSFORMATION

PM B 9108 Port Vila, Vanuatu
Tel: (678) 33380

GOUVERNEMENT DE LA REPUBLIQUE DU VANUATU

BUREAU DU PREMIER MINISTRE

CERTVU

DEPARTMENT DE COMMUNICATION ET DE TRANSFORMATION NUMERIQUE

SPP 9108 Port Vila, Vanuatu
Tel: (678) 33380

2 April 2026

Advisory 125: Cisco Secure Firewall Management Center (FMC) Software and Cisco Security Cloud Control (SCC) Firewall Management Deserialization of Untrusted Data Vulnerability

Release Date: 19th March 2026
Impact: HIGH / CRITICAL
TLP: CLEAR

Communication and Digital Transformation (DCDT through CERT Vanuatu (CERTVU), provides the following advisory.

This alert is relevant to Organizations and System/Network administrators that utilize the above products. This alert is intended to be understood by technical users and systems administrators.

What is it?

CVE-2026-20131 is a critical remote code execution (RCE) vulnerability (CVSS 10.0) affecting Cisco firewall management systems. The flaw is caused by insecure deserialization of untrusted data (CWE-502) in the web-based management interface.

Specifically, the application improperly processes user-supplied Java serialized objects**,** allowing attackers to inject malicious payloads that execute during deserialization.

What are the systems affected?

The Vulnerability impacts:

- Cisco Secure Firewall Management Center (FMC) Software
- Cisco Security Cloud Control (SCC) Firewall Management (related platform)

These systems are used to:

- Centrally manage enterprise firewalls
- Monitor network traffic and threats
- Enforce security policies across networks

Because FMC systems typically have high privileges and visibility across enterprise networks, compromise can have widespread impact.

What does this mean?

Attackers exploit CVE-2026-20131 through the exposed web interface.

Typical exploitation flow:

1. Target discovery
   - Attackers scan for exposed Cisco FMC management interfaces.
2. Crafted malicious payload
   - A specially crafted serialized Java object is created.
3. Delivery via HTTP request
   - The payload is sent to the vulnerable web interface endpoint.
4. Unsafe deserialization
   - The system processes the malicious object without validation.
5. Remote code execution
   - The payload executes attacker-controlled Java code.
6. Privilege escalation
   - Code runs with root-level privileges on the device.

Successful exploitation may allow attackers to:

- Execute arbitrary code on the firewall management system
- Gain full root access to the device
- Disable or bypass security controls
- Deploy ransomware or persistent backdoors
- Conduct lateral movement across the network
- Exfiltrate sensitive network and security data

Mitigation process

CERTVU recommends the following:

1. Apply Cisco Security Updates (Critical)

- Upgrade immediately to patched versions released by Cisco (March 2026 advisory).

2. Restrict Management Interface Exposure

- Do not expose FMC web interfaces to the public internet.
- Restrict access via:
  - VPN
  - Internal network segmentation

Reducing exposure significantly lowers attack risk.

Reference

1. https://www.cisa.gov/known-exploited-vulnerabilities-catalog
2. https://www.cve.org/CVERecord?id=CVE-2026-20131

.