An Lárionad Náisiúnta Cibearshlándála
National Cyber Security Centre

NCSC #2604020232

NCSC Advisory

Cisco: Cisco Secure Firewall Management Center (FMC)

CVE-2026-20131

2nd, April 2026

STATUS: TLP:CLEAR

Recipients can spread this to the world, there is no limit on disclosure. Sources may use TLP:CLEAR when information carries minimal or no foreseeable risk of misuse, in accordance with applicable rules and procedures for public release. Subject to standard copyright rules, TLP:CLEAR information may be shared without restriction.

For more information on the Traffic Light Protocol, see https://www.first.org/tlp/. Please treat this document in accordance with the TLP assigned.

Description

CVE ID: CVE-2026-20131

Published: 2026-03-04

Vendor: Cisco

Product: Secure Firewall Management Center (FMC)

CVSS Score[1]: 10.0

Products Affected

Product	Version
Cisco Secure Firewall Management Center (FMC)	6.4.0.13 before 7.0.9
Cisco Secure Firewall Management Center (FMC)	7.0.0 before 7.0.9
Cisco Secure Firewall Management Center (FMC)	7.1.0 before 7.2.11
Cisco Secure Firewall Management Center (FMC)	7.3.0 before 7.4.6
Cisco Secure Firewall Management Center (FMC)	7.6.0 before 7.6.5
Cisco Secure Firewall Management Center (FMC)	7.7.0 before 7.7.12
Cisco Secure Firewall Management Center (FMC)	10.0.0 before 10.0.1

[1] https://www.first.org/cvss/

Impact

A vulnerability in the web-based management interface of Cisco Secure Firewall Management Center (FMC) Software could allow an unauthenticated, remote attacker to execute arbitrary Java code as root on an affected device.

This vulnerability is due to insecure deserialization of a user-supplied Java byte stream. An attacker could exploit this vulnerability by sending a crafted serialized Java object to the web-based management interface of an affected device. A successful exploit could allow the attacker to execute arbitrary code on the device and elevate privileges to root. Note: If the FMC management interface does not have public internet access, the attack surface that is associated with this vulnerability is reduced.

Common Weakness Enumeration (CWE)[2]: CWE-502: Deserialization of Untrusted Data

Known Exploited Vulnerability (KEV) catalog[3]: Yes

Used by Ransomware Operators: Yes

Recommendations

The NCSC strongly recommends installing updates for vulnerable systems with the highest priority, after thorough testing. Affected organisations should review the latest release notes and install the relevant updates from Cisco.

- https://nvd.nist.gov/vuln/detail/CVE-2026-20131
- https://www.cve.org/CVERecord?id=CVE-2026-20131
- https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-fmc-rce-NKhnULJh
- https://aws.amazon.com/blogs/security/amazon-threat-intelligence-teams-identify-interlock-ransomware-campaign-targeting-enterprise-firewalls/
- https://www.cisa.gov/known-exploited-vulnerabilities-catalog?field_cve=CVE-2026-20131

[2] https://cwe.mitre.org
[3] https://www.cisa.gov/known-exploited-vulnerabilities-catalog