CYBER ADVISORY

Thursday, March 05, 2026 **CSIC-ADVISORY-202603-A-001**

Cisco Secure Firewall Management Center Vulnerabilities

Root Access	Insecure Deserialization	Crafted HTTP Requests	Privilege Escalation

The California Cybersecurity Integration Center (Cal-CSIC) has identified two critical vulnerabilities impacting the web-based management interface of Cisco's Secure Firewall Management Center. CVE-2026-20079 carries a CVSS 3.1 score of 10.0.[1] The vulnerability is due to an improper system process that is created at boot time that can be exploited by sending crafted HTTP requests to a targeted device.

Successful exploitation would allow an unauthenticated remote attacker to execute script files on an affected device to obtain root access to the underlying operating system. This vulnerability affects Cisco Secure FMC software regardless of device configuration, and there are no known workarounds that will address this vulnerability.[2] CVE-2026-20079 has not been confirmed to be exploited in the wild or as a zero-day vulnerability.

The second vulnerability, CVE-2026-20131, carries a CVSS 3.1 score of 10.0.[3] This vulnerability is due to insecure deserialization of a user-supplied java byte stream that can be exploited by sending a crafted serialized Java object to the web-based management interface of the targeted device.[4] Successful exploitation would allow an unauthenticated remote attacker to execute arbitrary code on a targeted device and elevate privileges to root.[5] CVE-2026-20131 has not been confirmed to be exploited in the wild or as a zero-day vulnerability.

Cisco has issued security advisories for each vulnerability with instructions to upgrade to fixed software.

The Cal-CSIC recommends immediately following the vendor's guidance to patching vulnerable systems. For further information on Cisco's security advisories and analysis please use these links:

Security Advisory

CVE-2026-20079
https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-onprem-fmc-authbypass-5JPp45V2

CVE-2026-20131

https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-fmc-rce-NKhnULJh

Affected Products:

- **CVE-2026-20131** affects Cisco Secure FMC Software and Cisco Security Cloud Control Firewall Management regardless of device configuration.

Analyst Comment: Cisco SCC Firewall Management is a SaaS-delivered offering and is upgraded by Cisco as part of maintenance – no user action is required.

- **CVE-2026-20079** affects Cisco Secure FMC Software regardless of device configuration.

References

[1] NVD; "CVE-2026-20079 Detail"; https://nvd.nist.gov/vuln/detail/CVE-2026-20079; accessed 05 March 2026
[2] Cisco; "Cisco Secure Firewall Management Center Software Authentication Bypass Vulnerability https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-onprem-fmc-authbypass-5JPp45V2; accessed 05 March 2026
[3] NVD; "CVE-2026-20131 Detail"; https://nvd.nist.gov/vuln/detail/cve-2026-20131; accessed 05 March 2026
[4] Tenable; "CVE-2026-20131"; https://www.tenable.com/cve/CVE-2026-20131; accessed 05 March 2026
[5] Cisco; "Cisco Secure Firewall Management Center Software Remote Code Execution Vulnerability"; https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-fmc-rce-NKhnULJh; accessed 05 March 2026