



## ADV2026\_205 Cisco Security Advisory (2<sup>nd</sup>, April 2026)

Cisco published a security advisory highlighting vulnerabilities in the following products on April 1st, 2026. It is recommended that you take the necessary precautions by ensuring your products are always updated.

- Cisco NFVIS Release – multiple versions
- Cisco IMC Release – multiple versions
- Cisco Telemetry Broker Appliances – version 6.0(2.260044) (M6) and prior
- IEC6400 Edge Compute Appliances – version 4.3(6.260017) (M6) and prior
- Secure Endpoint Private Cloud Appliances – versions 4.3(2.260007) (M5) and 4.3(6.260017) (M6)
- Secure Firewall Management Center Appliances – versions 4.3(2.260007) (M5) and 4.3(6.260017) (M6)
- Secure Malware Analytics Appliances – versions 4.3(2.260007) (M5) and 4.3(6.260017) (M6)
- Secure Network Analytics Appliances – versions 4.3(2.260007) (M5) and 6.0(2.260044) (M6)
- Secure Network Server Appliances – multiple versions
- Cisco SSM On-Prem Release – version 9-202510 and prior
- Cisco EPNM Release – versions 8.0 and prior, version 8.1 and prior

For more information on these updates, you can follow these URLs:

- [Cisco Integrated Management Controller Command Injection and Remote Code Execution Vulnerabilities](#)
- [Cisco Smart Software Manager On-Prem Privilege Escalation Vulnerability](#)
- [Cisco Evolved Programmable Network Manager Improper Authorization Vulnerability](#)
- [Cisco Integrated Management Controller Authentication Bypass Vulnerability](#)
- [Cisco Smart Software Manager On-Prem Arbitrary Command Execution Vulnerability](#)
- [Cisco Security Advisories](#)

The Guyana National CIRT recommends that users and administrators review these updates and apply them where necessary.



# CIRT.GY

Guyana National Computer Incident Response Team

## References

- Cisco Security advisories. (April 1<sup>st</sup>, 2026). Retrieved from Cisco <https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-cssm-priv-esc-xRAnOuO8>
- Cisco Security advisories. (April 1<sup>st</sup>, 2026). Retrieved from Canadian Centre for Cyber Security <https://www.cyber.gc.ca/en/alerts-advisories>