



# CIRT.GY

Guyana National Computer Incident Response Team

## **ADV2026\_190 Cisco Security Advisory (March 25th, 2026)**

Cisco published a security advisory highlighting vulnerabilities in the following products on March 25, 2026. It is recommended that you take the necessary precautions by ensuring your products are always updated.

- Cisco Catalyst 9300 Series Switches
- Cisco Catalyst 9200 Series Switches
- Cisco Catalyst 9000 Series Switches
- Cisco Catalyst ESS9300 Embedded Series Switches
- Cisco IOS Software
- Cisco IOS XE Software
- Cisco Secure Firewall ASA Software
- Cisco Secure FTD Software
- Cisco Catalyst IE9310 and IE9320 Rugged Series Switches
- Cisco IE3500 and IE3505 Rugged Series Switches
- Cisco Catalyst CW9800H Wireless Controllers
- Cisco Catalyst CW9800M Wireless Controllers
- Cisco Catalyst CW9800H1 Wireless Controllers
- Cisco Meraki MS390
- Cisco Catalyst SD-WAN Manager

For more information on these updates, you can follow this URL:

- [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 Advisory (March 25<sup>th</sup>, 2026). Retrieved from Cisco. <https://sec.cloudapps.cisco.com/security/center/viewErp.x?alertId=ERP-75297>
- Cisco Security Advisory (March 25<sup>th</sup>, 2026). Retrieved from Canadian Centre for Cyber Security. <https://www.cyber.gc.ca/en/alerts-advisories/cisco-security-advisory-av26-281>