



CIRT.GY

Guyana National Computer Incident Response Team

ADV2025_379 Cisco Security Advisory (October 16th, 2025)

Cisco published a security advisory highlighting vulnerabilities in the following product on October 15th, 2025. It is recommended that you take the necessary precautions by ensuring your product is always updated.

- Cisco TelePresence CE on-premises – versions 9, 10 and versions prior to 11.32.2.1
- Cisco RoomOS Release on-premises – versions 9, 10 and versions prior to 11.32.2.1
- Cisco RoomOS Release cloud-aware – versions prior to July 2025
- Cisco Open Source Snort 3 – versions prior to 3.9.3.0
- Cisco Desk Phone 9800 Series – versions prior to 3.3(1)
- Cisco IP Phone 7800 and 8800 Series – versions prior to 14.4(1)
- Cisco IP Phone 8821 – versions prior to 11.0(6)SR7
- Cisco Video Phone 8875 – versions prior to 3.3(1)

For more information on this update, you can follow these URLs:

- [Cisco TelePresence Collaboration Endpoint and RoomOS Software Information Disclosure Vulnerability](#)
- [Multiple Cisco Products Snort 3 MIME Denial of Service Vulnerabilities](#)
- [Cisco Desk Phone 9800 Series, IP Phone 7800 and 8800 Series, and Video Phone 8875 with SIP Software Vulnerabilities](#)
- [Cisco Security Advisories](#)

The Guyana National CIRT recommends that users and administrators review this update and apply it where necessary.

References

- Cisco Security Advisory (October 15th, 2025). Retrieved from Cisco <https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-roomos-inf-disc-qGgsbxAm>
- Cisco Security Advisory. (October 15th, 2025). Retrieved from Canadian Centre for Cyber Security. <https://www.cyber.gc.ca/en/alerts-advisories/cisco-security-advisory-av25-672>