ADV2025_182 Cisco Security Advisory (July 3rd, 2025)

Cisco has published a security advisory highlighting vulnerabilities in the following products on July 2nd, 2025. It is recommended that you take the necessary precautions by ensuring your products are always updated.

- Cisco BroadWorks Application Delivery Platform – versions prior to RI.2025.05
- Cisco Enterprise Chat and Email – version 11 and versions prior to 12.6(1)_ES11
- Cisco Spaces Connector – versions prior to Connector 3-Jun 2025
- Cisco Unified Communications Manager – versions 15.0.1.13010-1 to 15.0.1.13017-1
- Cisco Unified Communications Manager Session Management Edition Engineering Special (ES) – versions 15.0.1.13010-1 to 15.0.1.13017-1

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

Cisco BroadWorks Application Delivery Platform Cross-Site Scripting Vulnerability

Cisco Enterprise Chat and Email Stored Cross-Site Scripting Vulnerability

Cisco Spaces Connector Privilege Escalation Vulnerability

Cisco Unified Communications Manager Static SSH Credentials Vulnerability

Cisco Security Advisories

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

References

- Cisco Security Advisories. (July 2nd, 2025). Retrieved from Cisco. https://tools.cisco.com/security/center/publicationListing.x

- Cisco Security Advisory. (July 2nd, 2025). Retrieved from Canadian Centre for Cyber Security. https://www.cyber.gc.ca/en/alerts-advisories/cisco-security-advisory-av25-388