CIRT.GY Guyana National Computer Incident Response Team

ADV2024_30 Cisco Security Advisory (9th February 2024)

Cisco has published a security advisory to address vulnerabilities affecting the following products on February 7, 2024. It is recommended that you take the necessary precautions to ensure your products are always protected.

- Cisco Expressway Series – versions prior to 14.3.4
- Secure Endpoint Connector for Windows – versions prior to 7.5.17 and 8.2.1
- Secure Endpoint Private Cloud – versions prior to 3.8.0

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

1. Cisco Expressway Series Cross-Site Request Forgery Vulnerabilities
2. ClamAV OLE2 File Format Parsing Denial of Service Vulnerability in Secure Endpoint

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

References

- Cisco Security Advisories. (2024, February 7). Retrieved from Cisco. https://sec.cloudapps.cisco.com/security/center/publicationListing.x
- Cisco security advisory. (2024, February 7). Retrieved from Canadian Centre for Cyber Security. https://www.cyber.gc.ca/en/alerts-advisories/cisco-security-advisory-av24-072