ADV2024_243 Cisco Security Advisory (18th July 2024)

Cisco has published a security advisory to address vulnerabilities affecting the following products on July 17, 2024. It is recommended that you take the necessary precautions to ensure your products are always protected.

- Cisco AsyncOS for Secure Web Appliance – versions 14.5, 15.0 and 15.1
- Cisco Secure Email Gateway – Content Scanner Tools versions prior to 23.3.0.4823
- Cisco Smart Software Manager On-Prem (SSM On-Prem) – version 8-202206 and prior

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

1. Cisco Secure Web Appliance Privilege Escalation Vulnerability
2. Cisco Secure Email Gateway Arbitrary File Write Vulnerability
3. Cisco Smart Software Manager On-Prem Password Change Vulnerability

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

References

- Cisco Security Advisories. (2024, July 17). Retrieved from Cisco. https://sec.cloudapps.cisco.com/security/center/publicationListing.x
- Cisco security advisory. (2024, July 16). Retrieved from Canadian Centre for Cyber Security. https://www.cyber.gc.ca/en/alerts-advisories/cisco-security-advisory-av24-404