ADV2024_71 Fortinet Security Advisory (13th March 2024)

Fortinet has published a security advisory to address vulnerabilities affecting the following products on March 12, 2024. It is recommended that you take the necessary precautions to ensure your products are always protected.

- FortiClientEMS 7.2 – versions 7.2.0 to 7.2.2
- FortiClientEMS 7.0 – versions 7.0.1 to 7.0.10
- FortiClientEMS 6.4 – all versions
- FortiClientEMS 6.2 – all versions
- FortiClientEMS 6.0 – all versions
- FortiManager – multiple versions
- FortiOS 7.4 – versions 7.4.0 to 7.4.1
- FortiOS 7.2 – versions 7.2.0 to 7.2.5
- FortiOS 7.0 – versions 7.0.0 to 7.0.12
- FortiOS 6.4 – versions 6.4.0 to 6.4.14
- FortiOS 6.2 – versions 6.2.0 to 6.2.15
- FortiPAM 1.1 – all versions
- FortiPAM 1.0 – all versions
- FortiProxy 7.4 – version 7.4.0
- FortiProxy 7.2 – versions 7.2.0 to 7.2.6
- FortiProxy 7.0 – versions 7.0.0 to 7.0.12
- FortiProxy 2.0 – versions 2.0.0 to 2.0.13
- FortiSwitchManager 7.2 – versions 7.2.0 to 7.2.2
- FortiSwitchManager 7.0 – versions 7.0.0 to 7.0.2

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

1. FortiClientEMS - CSV injection in log download feature
2. FortiClientEMS - Pervasive SQL injection in DAS component
3. FortiOS & FortiProxy - Out-of-bounds Write in captive portal
4. FortiWLM MEA for FortiManager - improper access control in backup and restore features

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

References

- PSIRT Advisories. (2024, March 12). Retrieved from FortiGuard Labs. https://www.fortiguard.com/psirt
- Fortinet security advisory. (2024, March 12). Retrieved from Canadian Centre for Cyber Security. https://www.cyber.gc.ca/en/alerts-advisories/fortinet-security-advisory-av24-138