ADV2024_102 Fortinet Security Advisory (10th April 2024)

Fortinet has published a security advisory to address vulnerabilities affecting the following products on April 9, 2024. It is recommended that you take the necessary precautions to ensure your products are always protected.

- FortiClientLinux 7.2 – version 7.2.0
- FortiClientLinux 7.0 – versions 7.0.6 to 7.0.10
- FortiClientLinux 7.0 – versions 7.0.3 to 7.0.4
- FortiClientMac 7.2 – versions 7.2.0 to 7.2.3
- FortiClientMac 7.0 – versions 7.0.6 to 7.0.10
- FortiOS – multiple versions
- FortiProxy – multiple versions
- FortiSandbox 4.4 – versions 4.4.0 to 4.4.3
- FortiSandbox 4.2 – versions 4.2.0 to 4.2.6
- FortiSandbox 4.0 – versions 4.0.0 to 4.0.4

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

1. [FortiClient Linux] Remote Code Execution due to dangerous nodejs configuration
2. FortiClientMac - Lack of configuration file validation
3. FortiSandbox - Arbitrary file delete on endpoint
4. FortiSandbox - OS command injection on endpoint
5. FortiOS & FortiProxy - administrator cookie leakage

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

References

- PSIRT Advisories. (2024, April 9). Retrieved from FortiGuard Labs. https://www.fortiguard.com/psirt
- Fortinet security advisory. (2024, April 9). Retrieved from Canadian Centre for Cyber Security. https://www.cyber.gc.ca/en/alerts-advisories/fortinet-security-advisory-av24-190