ADV2026_145 Fortinet Security Advisory (March 11th, 2026)

Fortinet published a security advisory highlighting vulnerabilities in the following products on March 10, 2026. It is recommended that you take the necessary precautions by ensuring your products are always updated.

- FortiClientLinux 7.4 – versions 7.4.0 to 7.4.4
- FortiClientLinux 7.2 – versions 7.2.2 to 7.2.12
- FortiManager 7.4 – versions 7.4.0 to 7.4.2
- FortiManager 7.2 – versions 7.2.0 to 7.2.10
- FortiManager 6.4 – all versions
- FortiSwitchAXFixed 1.0 – versions 1.0.0 to 1.0.1
- FortiWeb 8.0 – versions 8.0.0 to 8.0.2
- FortiWeb 7.6 – versions 7.6.0 to 7.6.5
- FortiWeb 7.4 – versions 7.4.0 to 7.4.10
- FortiWeb 7.2 – versions 7.2.0 to 7.2.11
- FortiWeb 7.0 – versions 7.0.0 to 7.0.11

For more information on this update, you can follow this URL:

- Fortinet PSIRT Advisories

The Guyana National CIRT recommends that users and administrators review this update and apply it where necessary.

References

- Fortinet Security Advisory (March 10th, 2026). Retrieved from Fortinet. https://www.fortiguard.com/psirt?filter=1&version=&severity=5&severity=4&severity=3&severity=2
- Fortinet Security Advisory. (March 10th, 2026). Retrieved from Canadian Centre for Cyber Security. https://cyber.gc.ca/en/alerts-advisories/fortinet-security-advisory-av26-216