



ADV2026_195 Fortinet Security Advisory – Update 1

(March 31st, 2026)

Fortinet published a security advisory highlighting vulnerabilities in the following product on February 6th, 2026. It is recommended that you take the necessary precautions by ensuring your product is always updated.

- FortiClientEMS 7.4 – version 7.4.4

For more information on this update, you can follow these URLs:

- [SQLi in administrative interface – FG-IR-25-1142 \(CVE-2026-21643\)](#)
- [CWE-89: Improper Neutralization of Special Elements used in an SQL Command \('SQL Injection'\)](#)
- [Fortinet PSIRT Advisories](#)

Update 1

Open-source reporting indicates that CVE-2026-21643 is being exploited in the wild.

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

References

- SQLi in administrative interface – FG-IR-25-1142 (CVE-2026-21643). (February 06, 2026). Retrieved from FortiGuard Labs. <https://www.fortiguard.com/psirt/FG-IR-25-1142>
- CWE-89: Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection'). (n.b.). Retrieved from Fortinet. <https://cwe.mitre.org/data/definitions/89.html>
- Fortinet PSIRT Advisories. (n.b.). Retrieved from Fortinet. <https://www.fortiguard.com/psirt?filter=1&version=&severity=5&severity=4&severity=3&severity=2>



CIRT.GY

Guyana National Computer Incident Response Team

- Fortinet security advisory. (March 30, 2026). Retrieved from Canadian Centre for Cyber Security. <https://www.cyber.gc.ca/en/alerts-advisories/fortinet-security-advisory-av26-096>