

FOR IMMEDIATE RELEASE

October 22, 2026

Limehawk Urges Fortinet FortiOS Users to Update After CISA Lists Flaw as Exploited

CISA added the medium-severity Fortinet flaw to its Known Exploited Vulnerabilities catalog on Oct. 16. It requires a read-write admin login, and fixes have been out since April.

KNOXVILLE, Tenn., Oct. 22, 2026. Limehawk, LLC, a Knoxville managed IT services provider, today urged businesses that run Fortinet FortiOS, FortiProxy, FortiPAM or FortiSwitchManager to confirm they are on a fixed version, after the Cybersecurity and Infrastructure Security Agency (CISA) added CVE-2025-61624 to its Known Exploited Vulnerabilities (KEV) catalog.

CISA added the flaw on Oct. 16, 2026, "based on evidence of active exploitation," and gave federal civilian agencies until Oct. 19 to act. Its catalog lists known ransomware use as "Unknown." Fortinet rates the flaw Medium, with a CVSSv3 score of 6.0, and its advisory, FG-IR-26-122, now shows "Known Exploited: Yes." NVD scores it 6.5, also Medium. Fortinet first published the advisory and fixes on April 14, 2026. Neither the KEV entry nor Fortinet's advisory describes the attacks.

What is the flaw?

Fortinet describes a path traversal in the command line interpreter that "may allow a privileged attacker to achieve arbitrary write or delete files via specifically crafted arguments to existing commands." Fortinet lists the impact as escalation of privilege.

Who can exploit it?

Only someone who is already logged in as an administrator. NVD's description, provided by Fortinet, says it applies to "an authenticated attacker with admin profile and at least read-write permissions," and Fortinet lists the attack type as "Authenticated." In plain terms, an attacker needs a read-write admin login on the device before they can use this flaw.

Which versions are affected?

Fortinet lists these affected versions and fixes:

- FortiOS 7.6.0 through 7.6.4: upgrade to 7.6.5 or above.
- FortiOS 7.4.0 through 7.4.9: upgrade to 7.4.10 or above.
- FortiOS 7.2, 7.0 and 6.4, all versions: migrate to a fixed release.
- FortiProxy 7.6.0 through 7.6.4: upgrade to 7.6.5 or above.
- FortiProxy 7.4.0 through 7.4.11: upgrade to 7.4.12 or above.

- FortiProxy 7.2 and 7.0, all versions: migrate to a fixed release.
- FortiPAM 1.7.0: upgrade to 1.7.1 or above.
- FortiPAM 1.0 through 1.6, all versions: migrate to a fixed release.
- FortiSwitchManager 7.2.0 through 7.2.7: upgrade to 7.2.8 or above.
- FortiSwitchManager 7.0.0 through 7.0.6: upgrade to 7.0.7 or above.

Fortinet says FortiPAM 1.8 is not affected.

What should businesses do?

Limehawk recommends these steps:

- **Check the version.** Find every FortiOS, FortiProxy, FortiPAM and FortiSwitchManager device you or your IT provider runs, and compare its version to Fortinet's list.
- **Upgrade.** Install the fixed release for your branch. Fortinet says to follow its recommended upgrade path using its upgrade tool. FortiOS 7.2, 7.0 and 6.4 have no fix in those branches, so those devices need to move to a fixed release.
- **Review admin accounts.** Because the flaw needs a read-write admin login, check each device's administrator list, remove accounts you don't recognize or no longer need, and change the passwords on the rest.
- **Review management access.** Check which people and networks can reach each device's management interface and CLI, and limit it to those that need it.
- **Know about the virtual patch.** Fortinet says a virtual patch named FG-VD-59270.0day is available in FMWP db update 25.120. Upgrading is still the fix.

Sources

1. Fortinet PSIRT, "Path Traversal in CLI." FG-IR-26-122, published Apr. 14, 2026.
<https://fortiguard.fortinet.com/psirt/FG-IR-26-122>
2. CISA, "CISA Adds Two Known Exploited Vulnerabilities to Catalog." Oct. 16, 2026.
<https://www.cisa.gov/news-events/alerts/2026/10/16/cisa-adds-two-known-exploited-vulnerabilities-catalog>
3. CISA, "Known Exploited Vulnerabilities Catalog." Entry for CVE-2025-61624, added Oct. 16, 2026.
<https://www.cisa.gov/known-exploited-vulnerabilities-catalog>
4. NIST NVD, "CVE-2025-61624 Detail." Published Apr. 14, 2026.
<https://nvd.nist.gov/vuln/detail/CVE-2025-61624>

Media Contact

Corey Watson, Managing Member
Limehawk, LLC
press@limehawk.io
<https://limehawk.io>

###