contact@namiq.io · namiq.io

NamiQ

SECURITY ADVISORY

Fortinet Multiple Products exploited

CVE-2025-61624 · on CISA's exploited list since 16 October 2026

Analysis Report

If you run FortiOS, FortiProxy, FortiPAM or FortiSwitchManager, act now: the CISA date has already passed. First find your version and who holds read-write admin accounts. If you run none of these …

PREPARED BY	NamiQ	DATE	1 November 2026
FACTS AS OF	1 November 2026	VERSION	1.0
SEVERITY	**Medium: CVSS 3.1 5.4**	STATUS	On CISA's exploited list; due 19 October 2026

NamiQ © 2026 NamiQ. All rights reserved. This document is the property of NamiQ. It may be shared unaltered, with attribution.
Companion article: namiq.io/insights/fortinet-multiple-products-cve-2025-61624

The bottom line

> *If you run FortiOS, FortiProxy, FortiPAM or FortiSwitchManager, act now: the CISA date has already passed. First find your version and who holds read-write admin accounts. If you run none of these, stop reading.*

At a glance

Fact	Detail
Product	Fortinet Multiple Products (CVE-2025-61624)
Severity	Medium: 5.4 (CVSS 3.1)
CISA	On its exploited list since 16 October 2026. Deadline for US federal agencies: 19 October 2026.
Chance of exploitation (EPSS)	0.01, the estimated chance in the next 30 days, as at 1 November 2026
Ransomware use	Not recorded by CISA. That is not the same as none.
Fixed in	FortiOS 7.6.5, 7.4.10; FortiProxy 7.6.5, 7.4.12; FortiPAM 1.7.1; FortiSwitchManager 7.2.8, 7.0.7 (vendor advisory, 14 April 2026). Older branches: migrate to a fixed release.
Who looks first	Anyone running FortiOS, FortiPAM, FortiProxy or FortiSwitchManager, first where several people hold admin accounts or where admin logins can be reached from outside.

Does this apply to you?

Answer in order. Stop at the first no.

Question	If no	If yes
Do you run FortiOS, FortiProxy, FortiPAM or FortiSwitchManager?	Nothing to do for this CVE.	Check the version (next question).
Is your version inside an affected range, or on 7.2, 7.0 or 6.4 (FortiOS), or FortiPAM 1.6 or older?	Nothing to do for this CVE. FortiPAM 1.8 is listed as not affected.	Plan the upgrade or migration now.
Can anyone besides trusted staff log in to the CLI with a read-write admin profile?	Exposure is lower, but still patch.	Remove or restrict those accounts today.

Is the admin login reachable from the internet or from untrusted networks?	Keep it that way while you patch.	Restrict it to a management network first.

What it is

An attacker who is already logged in as an administrator with at least read-write permissions can use crafted CLI commands to write or delete files of their choosing on the device. The attacker needs that admin login first.

Why it matters

The vendor rates this Medium, but it is listed as exploited. Our reading is that a file write or delete on a security device is useful to an attacker who already holds admin access: it can change what the device does or remove traces. The record does not say what was written or deleted in attacks. A modest score is no reason to delay.

What the vendor's advisory says

We read one page on fortiguard.fortinet.com. In short:

- The vendor's advisory (FG-IR-26-122, 14 April 2026) rates it Medium, CVSSv3 6.0, attack type authenticated, and marks it as known exploited.
- It says FortiOS 7.2, 7.0 and 6.4 are affected in all versions, with no fixed release in those branches: the advice is to migrate.
- FortiPAM 1.6 and earlier are affected in all versions; FortiPAM 1.7.0 is fixed in 1.7.1; FortiPAM 1.8 is not affected.
- The advisory says a virtual patch is available in database update 25.120, for customers who use that service.
- The advisory points to the vendor's upgrade tool for the recommended upgrade path.

Things people will get wrong

- "Medium score, so it can wait." The vendor marks it as known exploited and CISA lists it. The score does not describe that.
- "It needs a login, so it is not our problem." The login needed is an admin with read-write rights. The record does not say how attackers get one, so check who holds such accounts.
- "Our FortiOS is old but stable, so we are fine." The advisory lists FortiOS 7.2, 7.0 and 6.4 as affected in all versions and says to migrate.

The wording includes conditions the score may not show: the attacker must be logged in. Read the record before you decide it does not apply to you.

How we would triage it

This is our judgement.

The commands only read: they print a version or list what is installed. They come from general knowledge of this kind of product, not from the sources, so check them against the vendor's page before you run them. Words in capitals are for you to fill in.

Step 1: Find the versions you run

- List every FortiOS, FortiProxy, FortiPAM and FortiSwitchManager device and its version.
- Compare each against the fixed versions: older branches have no fix in-branch.

```
get system status
```

Step 2: Reduce who can use the CLI

- List admin accounts and remove any read-write profile that is not needed, since the flaw needs one.
- Limit admin login to a management network and trusted addresses.

```
show system admin
```

Step 3: Patch or migrate

- Upgrade to a fixed version, or migrate if your branch has none, using the vendor's upgrade path.
- If you cannot patch at once, ask whether the vendor's virtual patch (database update 25.120) applies to you.

Step 4: Check for signs of misuse

- Review admin logins and CLI activity for accounts or times you do not recognise.
- Look for files that were changed or are missing without a change request.

To close it, read the version from the product itself, not from an old inventory, and save the output with the date. If you cannot update today, write down who owns it, the new date, and what limits exposure until then.

Send this to your IT provider

Copy it, change the names and dates, and send it. It is a draft for you to check, not a template tested with any provider.

> *Hello. Please tell us whether we run FortiOS, FortiProxy, FortiPAM or FortiSwitchManager, and where. For each, please give the exact version. The vendor's advisory for CVE-2025-61624 lists fixed versions: FortiOS 7.6.5 or 7.4.10, FortiProxy 7.6.5 or 7.4.12, FortiPAM 1.7.1, FortiSwitchManager 7.2.8 or 7.0.7. Older branches need migration. CISA lists this flaw as exploited and its date has passed. Please also list who holds read-write admin accounts. Please confirm the version and the fix to us in writing by a date you propose this week. Thank you.*

Signs it was used

An update closes the hole. It does not tell you whether someone used it first. CISA's required action points to its forensic triage requirements (BOD 26-04). Look for:

- Admin logins at unusual times or from addresses you do not recognise.
- CLI commands run by admin accounts that no one can account for.
- Files on the device that have changed or disappeared without a planned change.

The weakness behind it

The record classes this as CWE-22 (Improper Limitation of a Pathname to a Restricted Directory).

The sources, in their words

CISA's catalogue entry:

> *FortiOS, FortiPAM, FortiProxy, and FortiSwitchManager contain a path traversal vulnerability that may allow an authenticated attacker with admin profile and at least read-write permissions to write or delete arbitrary files via specific CLI commands.*

The CVE record, published by Fortinet on 14 April 2026:

> *An Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') [CWE-22] vulnerability in Fortinet FortiOS 7.6.0 through 7.6.4, FortiOS 7.4.0 through 7.4.9, FortiOS 7.2 all versions, FortiOS 7.0 all versions, FortiOS 6.4 all versions, FortiPAM 1.7.0, FortiPAM 1.6 all versions, FortiPAM 1.5 all versions, FortiPAM 1.4 all versions, FortiPAM 1.3 all versions, FortiPAM 1.2 all versions, FortiPAM 1.1 all versions, FortiPAM 1.0 all versions, FortiProxy 7.6.0 through 7.6.4, FortiProxy 7.4.0 through 7.4.11, FortiProxy 7.2 all versions, FortiProxy 7.0 all versions, FortiSwitchManager 7.2.0 through 7.2.7, FortiSwitchManager 7.0.0 through 7.0.6 may allow an authenticated attacker ...*

Versions of Fortinet FortiOS the record lists as affected:

- 7.6.0 through 7.6.4
- 7.4.0 through 7.4.9
- 7.2.0 through 7.2.13
- 7.0.0 through 7.0.19
- 6.4.0 through 6.4.16

Versions of Fortinet FortiProxy the record lists as affected:

- 7.6.0 through 7.6.4
- 7.4.0 through 7.4.11
- 7.2.0 through 7.2.16
- 7.0.0 through 7.0.23

Versions of Fortinet FortiSwitchManager the record lists as affected:

- 7.2.0 through 7.2.7
- 7.0.0 through 7.0.6

Versions of Fortinet FortiPAM the record lists as affected:

- 1.7.0
- 1.6.0 through 1.6.2
- 1.5.0 through 1.5.1
- 1.4.0 through 1.4.3
- 1.3.0 through 1.3.1
- 1.2.0
- 1.1.0 through 1.1.2
- 1.0.0 through 1.0.3

CISA's required action:

> *Apply mitigations in accordance with vendor instructions, ensuring compliance with CISA's BOD 26-04 Prioritizing Security Updates Based on Risk (see URL in Notes) guidance and CISA's "Forensics Triage Requirements" (see URL in Notes).*

What we do not know yet

- Which files attackers wrote or deleted, and how they got the admin login, are not stated.
- No source names a fixed release for FortiOS 7.2, 7.0 or 6.4; the advice is only to migrate.
- The sources do not say whether the virtual patch fully blocks the flaw.

- The advisory says the flaw was found internally; the sources do not describe the attacks.
- We have not tested this against any environment. Versions and scores are as the sources state them and as at 1 November 2026; the vendor's advisory wins where it differs.
- The sections headed "The bottom line", "Does this apply to you?", "What it is", "Why it matters", "Exposure by situation", "Things people will get wrong", "How we would triage it" and "Send this to your IT provider" are our interpretation of the sources, not a statement by CISA or the vendor.

Appendix 1. Severity decoded

CVE-2025-61624: score 5.4, `CVSS:3.1/AV:L/AC:L/PR:H/UI:N/S:U/C:N/I:H/A:H/E:P/RL:O/RC:C` As the CVE record gives it. The record's own score can differ from the base score on the NVD record.

Metric	Value	What it means here
Attack vector	Local	Needs an account or code already running on the machine.
Attack complexity	Low	No special conditions beyond the flaw itself.
Privileges required	High	An administrator account is needed.
User interaction	None	No one has to do anything.
Scope	Unchanged	Damage stays inside the vulnerable component.
Confidentiality	None	No data exposed.
Integrity	High	Total loss of integrity.
Availability	High	Total loss of availability.

Appendix 2. Timeline

Date	Event
14 April 2026	CVE record published by Fortinet.
16 October 2026	CISA added it to its list of exploited vulnerabilities.
19 October 2026	CISA's deadline for US federal agencies.

Appendix 3. Exposure by situation

These priorities are our judgement from the attacker prerequisites in the sources. They are not vendor ratings.

Your situation	Priority	Timeframe
Affected version with admin login reachable from the internet	High	Now; the CISA window has passed
Affected version, admin access only from a management network	High	Now; CISA lists it as exploited
FortiOS 7.2, 7.0 or 6.4 with no fixed release in the branch	High	Now; plan migration and tighten admin access

Fixed version already installed	Low	Confirm in writing; no further action
No Fortinet products in your estate	None	None for this CVE

Appendix 4. Definition of done

- Every Fortinet Multiple Products you run is listed, with its version.
- Each is outside the affected list, or the vendor's mitigation is in place.
- The version output or a screenshot is saved with the date.
- Logs for the weeks before the update were searched, and anything odd was written down.
- Anything not done has an owner and a date.

Sources

- CISA Known Exploited Vulnerabilities catalogue: https://www.cisa.gov/known-exploited-vulnerabilities-catalog
- CVE record for CVE-2025-61624: https://www.cve.org/CVERecord?id=CVE-2025-61624
- FIRST: Exploit Prediction Scoring System: https://www.first.org/epss/
- Advisory or release notes read: fortiguard.fortinet.com/psirt/FG-IR-26-122: https://fortiguard.fortinet.com/psirt/FG-IR-26-122