contact@namiq.io · namiq.io

NamiQ

SECURITY ADVISORY

Palo Alto Networks PAN-OS exploited

CVE-2026-0322 · on CISA's exploited list since 14 October 2026

Analysis Report

Act now if you run PAN-OS firewalls or Panorama: CISA's deadline was 17 October 2026. First confirm the management interface is not reachable from the internet, then upgrade to a fixed version. If …

PREPARED BY	NamiQ	DATE	1 November 2026
FACTS AS OF	1 November 2026	VERSION	1.0
SEVERITY	**High: CVSS 4.0 8.6**	STATUS	On CISA's exploited list; due 17 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/palo-alto-networks-pan-os-cve-2026-0322

The bottom line

> *Act now if you run PAN-OS firewalls or Panorama: CISA's deadline was 17 October 2026. First confirm the management interface is not reachable from the internet, then upgrade to a fixed version. If you run no PAN-OS, you can stop reading.*

At a glance

Fact	Detail
Product	Palo Alto Networks PAN-OS (CVE-2026-0322)
Severity	High: 8.6 (CVSS 4.0)
CISA	On its exploited list since 14 October 2026. Deadline for US federal agencies: 17 October 2026.
Chance of exploitation (EPSS)	0.02, 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	PAN-OS 12.2.4, 12.1.10-h2, 11.2.16, 11.1.16-h3, 10.2.18-h12 or later; the vendor also lists earlier fixed hotfixes per branch.
Who looks first	Anyone running PAN-OS on PA-Series or VM-Series firewalls, or on Panorama (virtual or M-Series). The vendor says Cloud NGFW and Prisma Access are not affected.

Does this apply to you?

Answer in order. Stop at the first no.

Question	If no	If yes
Do you run PAN-OS on a PA-Series or VM-Series firewall, or on Panorama?	Nothing to do for this CVE.	Check the version (next question).
Is your PAN-OS version below the fixed version for its branch?	You have the fix. Keep management access restricted.	Upgrade to the fixed version for your branch.
Can the management interface be reached from the internet?	Risk is lower, but still patch.	Restrict it to a single jump box now, then patch.
Could an untrusted person hold or obtain an administrator login?	Risk is lower, but still patch.	Review and remove accounts, then patch.

What it is

An attacker who can log in to the management interface can run any code as root on the firewall. The record says the attacker needs network access and a login with high privileges. The weakness is code injection (CWE-94).

Why it matters

Our reading is that the login requirement protects you only if administrator accounts and management access are tightly held. The vendor says exploitation has been observed against the management interface, though it calls it very limited. A firewall guards the rest of the network, so root on it gives an attacker a strong position. The vendor says the risk is highest when the interface is open to the internet.

What the vendor's advisory says

We read one page on security.paloaltonetworks.com. In short:

- The vendor scores this 8.6 (HIGH) and suggests urgency HIGHEST. It says it found the issue internally.
- The vendor says no special configuration is needed to be affected.
- The vendor says very limited exploitation has been observed targeting the management interface.
- Workaround from the vendor: allow only a jump box to reach the management interface. It scores the residual risk 8.5.
- Example fix path from the vendor: 12.1.2 through 12.1.4-h* upgrades to 12.1.4-h12 or 12.1.10-h2 or later.

Things people will get wrong

- "It needs a login, so it can wait." The vendor says exploitation has been observed. An attacker with a login gets root on the firewall, so a stolen or weak login is enough.
- "We run it in the cloud, so we are covered." Only Cloud NGFW and Prisma Access are unaffected. VM-Series firewalls and virtual Panorama are affected.

The wording includes conditions the score may not show: it needs privileges; 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 PA-Series, VM-Series and Panorama device you run, virtual ones included.
- Read each software version and compare it with the fixed version for its branch.

```
show system info
```

Step 2: Reduce exposure

- Allow management access only from one jump box, as the vendor suggests.
- Confirm the management interface is not open to the internet.

Step 3: Patch

- Upgrade each device to the fixed version for its branch, for example 11.2.16 or 10.2.18-h12.
- The vendor says to remediate as soon as possible.

Step 4: Check for signs of misuse

- Review administrator accounts and recent management logins for anything you do not recognise.

```
show admins
```

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, we need to know whether we run Palo Alto Networks PAN-OS (PA-Series, VM-Series or Panorama) and, if so, where and on which version. This concerns CVE-2026-0322, a remote code execution flaw in the management interface that the vendor says has been attacked. Please tell us whether the management interface is reachable from the internet, and restrict it to a jump box if so. Fixed versions include 12.2.4, 12.1.10-h2, 11.2.16, 11.1.16-h3 and 10.2.18-h12. CISA's deadline was 17 October 2026. Please confirm in writing the version of each device and that the fix is installed, by a date we agree.*

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:

- Administrator accounts you did not create, or management logins from addresses you do not know.
- Configuration changes or commits that nobody on your side made.
- Unexpected outbound connections from the firewall itself.

The weakness behind it

The record classes this as CWE-94 (Improper Control of Generation of Code).

The sources, in their words

CISA's catalogue entry:

> *Palo Alto Networks PAN-OS contains a code injection vulnerability that could allow an authenticated attacker with network access to execute arbitrary code with root privileges on the firewall.*

The CVE record, published by Palo_alto on 14 October 2026:

> *A remote code execution (RCE) vulnerability in the management interface of Palo Alto Networks PAN-OS® software enables an authenticated attacker with network access to execute arbitrary code with root privileges on the firewall. The security risk posed by this issue is minimized by restricting access to the management interface to only trusted internal IP addresses according to our recommended best practice deployment guidelines https://live.paloaltonetworks.com/t5/community-blogs/tips-amp-tricks-how-to-secure-the-management-access-of-your-palo/ba-p/464431 . This issue is applicable to PAN-OS software on PA-Series and VM-Series firewalls and on Panorama (virtual and M-Series). Cloud NGFW ...*

It lists these as unaffected:

- All

Versions of Palo Alto Networks PAN-OS the record lists as affected:

- 12.2.0 up to, but not including, 12.2.4
- 12.1.0 up to, but not including, 12.1.10-h2
- 11.2.0 up to, but not including, 11.2.16
- 11.1.0 up to, but not including, 11.1.16-h3
- 10.2.0 up to, but not including, 10.2.18-h12

The affected ranges end before 12.2.4, 12.1.10-h2, 11.2.16, 11.1.16-h3, 10.2.18-h12. Those are the first versions the record does not list as affected; confirm them in the vendor's advisory.

It lists these as unaffected:

- All

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

- The sources do not say who is exploiting this, or how many devices are affected.
- The record does not say how an attacker would get the login the flaw requires.
- The advisory text available here is cut off, so some per-branch fixed versions are not shown.
- The sources give no indicators or log entries that show a device was exploited.
- 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-2026-0322: score 8.6, `CVSS:4.0/AV:N/AC:L/AT:N/PR:H/UI:N/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N/E:A/AU:N/R:U/V:D/RE:M/U:Red` 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	Network	Reachable over a network, with no need to be on the same segment.
Attack complexity	Low	No special conditions beyond the flaw itself.
Attack requirements	None	Works against a default deployment.
Privileges required	High	An administrator account is needed.
User interaction	None	No one has to do anything.
Vulnerable system: confidentiality	High	Total loss of confidentiality.
Vulnerable system: integrity	High	Total loss of integrity.
Vulnerable system: availability	High	Total loss of availability.
Subsequent systems: confidentiality	None	No data exposed.
Subsequent systems: integrity	None	Nothing can be altered.
Subsequent systems: availability	None	No effect on availability.

Appendix 2. Timeline

Date	Event
14 October 2026	CVE record published by Palo_alto.
14 October 2026	CISA added it to its list of exploited vulnerabilities.
17 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
Management interface open to the internet on a version below the fix	High	Immediately
Management interface limited to a trusted internal range, version below the fix	Medium	This week
Many people hold administrator logins, or logins are shared	Medium	This week, alongside patching
Version already at or above the fixed version for its branch	Low	Keep access restricted
No PAN-OS, or only Cloud NGFW or Prisma Access	None	None for this CVE

Appendix 4. Definition of done

- Every Palo Alto Networks PAN-OS 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-2026-0322: https://www.cve.org/CVERecord?id=CVE-2026-0322
- FIRST: Exploit Prediction Scoring System: https://www.first.org/epss/
- Advisory or release notes read: security.paloaltonetworks.com/CVE-2026-0322: https://security.paloaltonetworks.com/CVE-2026-0322