contact@namiq.io · namiq.io

NamiQ

SECURITY ADVISORY

Vates Xen Orchestra exploited

CVE-2026-133469 · on CISA's exploited list since 25 November 2026

Analysis Report

Anyone running Xen Orchestra below 6.9.2 (stable) or 6.10.1 (latest) must act by 28 November 2026 — three days away. Remove internet access to the web interface immediately, then update; active …

PREPARED BY	NamiQ	DATE	26 November 2026
FACTS AS OF	26 November 2026	VERSION	1.0
SEVERITY	**Critical: CVSS 3.1 9.8**	STATUS	On CISA's exploited list; due 28 November 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/vates-xen-orchestra-cve-2026-133469

The bottom line

> *Anyone running Xen Orchestra below 6.9.2 (stable) or 6.10.1 (latest) must act by 28 November 2026 — three days away. Remove internet access to the web interface immediately, then update; active exploitation is confirmed.*

At a glance

Fact	Detail
Product	Vates Xen Orchestra (CVE-2026-133469)
Severity	Critical: 9.8 (CVSS 3.1)
CISA	On its exploited list since 25 November 2026. Deadline for US federal agencies: 28 November 2026.
Chance of exploitation (EPSS)	0.01, the estimated chance in the next 30 days, as at 26 November 2026
Ransomware use	Not recorded by CISA. That is not the same as none.
Fixed in	xen-orchestra 6.9.2 (stable channel) and 6.10.1 (latest channel); xo-server 5.211.2 and 5.213.1. The vendor's advisory confirms fixes are released to both channels.
Who looks first	Anyone running Xen Orchestra or the Xen Orchestra Appliance below version 6.9.2 (stable) or 6.10.1 (latest). The record also lists xo-server versions below 5.211.2 and 5.213.1 as affected.

Does this apply to you?

Answer in order. Stop at the first no.

Question	If no	If yes
Do you run Xen Orchestra or the Xen Orchestra Appliance?	Nothing to do for this CVE.	Check the version (next question).
Is the version below 6.9.2 (stable channel) or below 6.10.1 (latest channel)?	Patching is complete; check for prior compromise if it was internet-exposed.	Update immediately; check whether it faces the internet (next question).
Is the Xen Orchestra web interface reachable from outside a dedicated management network?	Update within the CISA window; risk is lower but patching is still required.	Take it off the internet now, then update and check for signs of compromise.

What it is

An attacker who can reach the Xen Orchestra REST interface sends an authentication cookie containing an empty JSON object. The record says the token provider treats this as an unfiltered lookup, returns the first valid token it finds, and grants the sender administrative access with no password.

Why it matters

This flaw needs no login: anyone who can reach the REST interface can authenticate as an administrator in one request. The vendor's advisory says that leads to arbitrary code execution on managed pools and a full XCP-ng host takeover as root. Active exploitation is confirmed by the advisory. Our reading is that the three-day CISA window reflects how direct the exploit is — no credentials, no prior foothold. The advisory also notes there is no access log for the unauthenticated path, so a compromise may leave no trace in Xen Orchestra's own logs.

What the vendor's advisory says

We read three pages on docs.vates.tech and github.com. In short:

- The advisory (VSA-2026-062, published 10 November 2026) covers only this vulnerability; it lists no other CVEs in the same release.
- The advisory says fixes are available on the stable channel (6.9.2) and the latest channel (6.10.1) and recommends updating as soon as possible.
- The advisory recommends placing Xen Orchestra on a dedicated management network; blocking the attacker IP addresses it names is listed as an additional step to break the known kill chain.
- The advisory warns that a WAF rule blocking the empty-token pattern may be bypassed using other token formats; treat it as a supplement to patching, not a substitute.

Things people will get wrong

- No unusual log entries means no intrusion The vendor's advisory says there is no log for the unauthenticated access path; absence of log entries does not rule out compromise.
- Blocking the named IP addresses is sufficient to stop the threat The advisory says its detection methods cover only the known campaign; exploitation by other actors using different infrastructure cannot be ruled out.
- The attacker must already have an account to exploit this The CVSS string (PR:None, UI:None) and the record both say no privileges are required. The flaw bypasses authentication entirely; no prior account is needed.
- Only an internet-exposed instance is at risk CVSS scores this as network-reachable with no privileges required. Any host that can reach the REST interface over any network is a potential

attacker.

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

- Check whether xen-orchestra and xo-server are installed and note their versions. The record lists xen-orchestra below 6.9.2 or below 6.10.1, and xo-server below 5.211.2 or below 5.213.1, as affected.
- Check whether the Xen Orchestra Appliance is in use; the vendor's advisory lists it as affected.

```
cat /etc/xo-appliance/version
```

Step 2: Remove internet exposure

- The vendor's advisory recommends moving Xen Orchestra to a dedicated management network and blocking external access to its interface before updating.
- If immediate isolation is not possible, block the IP addresses listed in the advisory at the firewall; the advisory says this addresses only the known campaign.

Step 3: Update to the fixed version

- Update xen-orchestra to 6.9.2 (stable) or 6.10.1 (latest), and xo-server to 5.211.2 or 5.213.1. The vendor's advisory says fixes are released to both channels.
- Follow the vendor's standard upgrade procedure for the channel in use.

Step 4: Check for signs of compromise

- The vendor's advisory says the exploit can be detected by reviewing HTTP request logs for the patterns authenticationToken=j:%7B%7D or authenticationToken=j:{}; there is no log for the unauthenticated access itself.

- On XCP-ng hosts, the advisory says to search for a VM named pivot2 in running VMs and for the attacker-planted files it lists in /etc/cron.d/ and the filesystem root.

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. CISA's wording adds that you should stop using the product if no mitigation is available.

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.

> *We run Xen Orchestra and need to assess our exposure to CVE-2026-133469, a critical authentication-bypass flaw that CISA lists as actively exploited with a remediation deadline of 28 November 2026. Please confirm: (1) which version of xen-orchestra and xo-server is installed, (2) whether the Xen Orchestra web interface is reachable from outside our management network, and (3) whether we are already on version 6.9.2 (stable) or 6.10.1 (latest) for xen-orchestra, or the equivalent fixed xo-server versions. If not, we need the upgrade scheduled immediately. Please send written confirmation of the installed version and fix status by 27 November 2026.*

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:

- The vendor's advisory says review HTTP request logs for the patterns authenticationToken=j:%7B%7D or authenticationToken=j:{} to detect the specific exploit.
- On XCP-ng hosts, the advisory says to search for a VM named pivot2 in running VMs, and for the files /etc/cron.d/zz-ustar2, /etc/cron.d/zz-ustar, /.ustar5, and /.ustar6.
- The advisory says to check /etc/ld.so.preload on XCP-ng hosts; its presence or unexpected contents may indicate a host-level compromise.

The weakness behind it

The record classes this as CWE-287 (Improper Authentication) and CWE-1287 (Improper Validation of Specified Type of Input).

Likely ATT&CK mapping

MITRE ATT&CK is a public catalogue of the steps attackers take, from getting in to causing damage. No source has mapped this flaw to it yet, so the steps below are our prediction from what the record

says the flaw allows. They are not MITRE's, the vendor's or CISA's, and an attacker may do other things.

Steps an attacker would likely take with this flaw

The step, in plain words	Stage of an attack	Why we think so
Exploit Public-Facing Application (T1190): Breaking in through a service that faces the internet, such as a web server, VPN or login page.	Initial Access: getting in	The flaw is in a network-accessible REST interface requiring no authentication, which would likely serve as the initial access point for an attacker targeting an internet-facing instance.
Valid Accounts (T1078): Logging in with a real account the attacker should not have, so the activity looks like normal use.	Initial Access: getting in	After bypassing authentication, the record says the exploit returns reusable admin login token IDs; an attacker would likely reuse these tokens to maintain access as a valid token holder.
Escape to Host (T1611): Breaking out of a container to reach the machine that hosts it.	Privilege Escalation: gaining higher rights	The vendor's advisory says Xen Orchestra compromise leads to a full XCP-ng host takeover as root, which would typically represent an escape from the virtualisation management layer to the underlying host.

How to use this: ask your IT provider which control or log would show each step, for example whether sign-in attempts from the internet are recorded. If nobody can answer, that is the gap to close first.

MITRE ATT&CK® is a registered trademark of The MITRE Corporation. Technique names are MITRE's.

The sources, in their words

CISA's catalogue entry:

> *Vates Xen Orchestra contains an improper validation of specified type of input vulnerability that could allow an unauthenticated attacker to bypass authentication and perform actions with administrative privileges via a specially crafted authentication token containing an empty JSON object.*

The CVE record, published by GitHub on 23 November 2026:

> *XO (Xen Orchestra) is a solution to visualize, manage, backup and delegate your XCP-ng (or XenServer) infrastructure. Prior to 6.9.2 and 6.10.1, REST cookie parsing turns authenticationToken=j:%7B%7D into {}. REST authentication passes that object to the XO token provider without requiring a string. The token collection treats {} as an unfiltered lookup and returns its first token; the provider authenticates as that token's owner if it is unexpired. The authenticated /rest/v0/users/me/authentication_tokens route then returns reusable login token IDs. This vulnerability is actively exploited in the wild. This vulnerability is fixed in 6.9.2 and 6.10.1.*

Versions of vatesfr xen-orchestra the record lists as affected:

- < 6.9.2
- >= 6.10.0, < 6.10.1

Versions of xen-orchestra xo-server the record lists as affected:

- < 5.211.2
- >= 5.213.0, < 5.213.1

CISA's required action:

> *Apply mitigations in accordance with vendor instructions.*

Check your own project

If you build software, you can compare what a project declares with this CVE from a terminal. The tool reads requirements files, package.json, Maven, Gradle, Cargo, CMake and Dockerfile files, runs nothing, and only the CVE id leaves your machine. Naming the CVEs needs no key.

```
lattice-scan project . --cve CVE-2026-133469
```

Each row says in-range, outside-range, undetermined or lead, with the file and line. That is evidence about what a manifest declares, not about what runs, and a person decides. The verdicts, the CSV columns and a pipeline recipe are in the guide.

Check the servers you run

The same id can be checked against a host. Run this on the machine itself, not on the laptop that deploys to it: it reads installed packages (dpkg, rpm or apk), snaps, the hardware (maker, model, firmware), the running container images with their operating system and packages, and the kernel version, compares them on the spot, and only the CVE ids leave the machine; the inventory stays on

it, in ~/.lattice-scan. Naming the CVEs needs no key. Do it on each server after a deployment, and again when a new entry lands.

```
lattice-scan --cve CVE-2026-133469
```

A match is a candidate for a person to confirm, not a finding. A distribution can fix a CVE under an unchanged version number, so a match is a candidate; on Debian-family hosts the report also shows whether the package's own changelog names the CVE. By default it opens the images your containers are running and reads their operating system and package list; a deep scan (--deep, a few minutes) opens every local image and the Python, Node, Java and Ruby packages inside them; for what an image declares, use the project check on its Dockerfile.

Guide: namiq.io/lattice/guides/choose-your-channel. MCP server (io.namiq/lattice in the MCP registry): namiq.io/lattice. Package: pypi.org/project/lattice-scan, or namiq.io/apt.

What we do not know yet

- The CVSS 4.0 score has not been published; the vendor's advisory notes it is not yet available.
- The record does not say whether the fixed versions require a restart of managed VMs or XCP-ng hosts.
- The sources do not describe whether the token returned by the exploit is always tied to the same admin account or varies by installation.
- The advisory says its detection methods cover only the known campaign; it does not describe what other exploitation patterns might look like.
- We have not tested this against any environment. Versions and scores are as the sources state them and as at 26 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", "Likely ATT&CK mapping", "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-2026-133469: score 9.8, `CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H` 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.
Privileges required	None	No account is needed.
User interaction	None	No one has to do anything.
Scope	Unchanged	Damage stays inside the vulnerable component.
Confidentiality	High	Total loss of confidentiality.
Integrity	High	Total loss of integrity.
Availability	High	Total loss of availability.

Appendix 2. Timeline

Date	Event
23 November 2026	CVE record published by GitHub.
25 November 2026	CISA added it to its list of exploited vulnerabilities.
28 November 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
Xen Orchestra internet-exposed and running a version below 6.9.2 or 6.10.1	High	Immediately — active exploitation is confirmed
Xen Orchestra on an internal network only but running an affected version	High	By 28 November 2026 (CISA deadline)
Updated to 6.9.2 or 6.10.1 but no post-compromise check done and it was internet-facing	Medium	This week

Patched and always on a dedicated management network, never internet-exposed	Low	Next patch cycle; verify advisory IoCs as a precaution
Not running Xen Orchestra or the Xen Orchestra Appliance	None	None for this CVE

Appendix 4. Definition of done

- Every Vates Xen Orchestra 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.
- Your projects' declared dependencies were checked against this CVE, and every row has a written reason.
- 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-2026-133469: https://www.cve.org/CVERecord?id=CVE-2026-133469
- FIRST: Exploit Prediction Scoring System: https://www.first.org/epss/
- Advisory or release notes read: docs.vates.tech/security-advisories/advisories/2026/vates-sa-20: https://docs.vates.tech/security-advisories/advisories/2026/vates-sa-2026-062/
- Advisory or release notes read: docs.vates.tech/security-advisories/advisories/2026/vates-sa-20: https://docs.vates.tech/security-advisories/advisories/2026/vates-sa-2026-062/
- Advisory or release notes read: github.com/vatesfr/xen-orchestra/security/advisories/GHSA-: https://github.com/vatesfr/xen-orchestra/security/advisories/GHSA-2r3w-c2vx-fv5g
- Reference in the CVE record: github.com: https://github.com/vatesfr/xen-orchestra/pull/10748
- Reference in the CVE record: github.com: https://github.com/vatesfr/xen-orchestra/commit/50166fe3a49c02069d35ba9046ca4a1f77f4e11d
- Reference in the CVE record: docs.vates.tech: https://docs.vates.tech/security-advisories/advisories/2026/vates-sa-2026-062