contact@namiq.io · namiq.io

NamiQ

SECURITY ADVISORY

OpenIdentityPlatform OpenAM: new CVE

CVE-2026-123551 · record published 8 November 2026

Analysis Report

Organisations not running OpenIdentityPlatform OpenAM can stop reading. Those on versions 14.0.0 to 16.1.3 must upgrade to 16.1.4 promptly — the record scores this 10.0 and no login is needed to ...

PREPARED BY	NamiQ	DATE	8 November 2026
FACTS AS OF	8 November 2026	VERSION	1.0
SEVERITY	**Critical: CVSS 4.0 10.0**	STATUS	Not on CISA's exploited list; exploitation not recorded

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/openidentityplatform-openam-cve-2026-123551

The bottom line

> *Organisations not running OpenIdentityPlatform OpenAM can stop reading. Those on versions 14.0.0 to 16.1.3 must upgrade to 16.1.4 promptly — the record scores this 10.0 and no login is needed to exploit it. Verify the installed version first.*

At a glance

Fact	Detail
Product	OpenIdentityPlatform OpenAM (CVE-2026-123551)
Severity	Critical: 10 (CVSS 4.0)
Status	A new CVE record, published by VulnCheck on 8 November 2026. Not on CISA's list of exploited vulnerabilities when we read it on 8 November 2026, which means nothing public says yet that anyone is using it.
Fixed in	OpenAM 16.1.4 — packages openam-federation-library, openam-notifications-websocket, and openam-server-only (advisory GHSA-5c3q-hp86-xjr8, published 22 October 2026).
Who looks first	Teams running OpenIdentityPlatform OpenAM as an identity or single sign-on provider on any version from 14.0.0 through 16.1.3, particularly where the server port is reachable from untrusted networks.

Does this apply to you?

Answer in order. Stop at the first no.

Question	If no	If yes
Do you run OpenIdentityPlatform OpenAM?	Nothing to do for this CVE.	Check the installed version (next question).
Is the installed version between 14.0.0 and 16.1.3 inclusive?	16.1.4 is the first unaffected version; no action needed.	Check whether the OpenAM port is reachable by untrusted clients.
Can untrusted users or systems reach the OpenAM port on the network?	Upgrade is still advisable; isolation reduces the immediate exposure.	Treat as urgent and upgrade to 16.1.4 without delay.

What it is

An unauthenticated attacker who can reach the OpenAM port connects to its notification WebSocket via a bypass on a legacy Liberty ID-FF endpoint. From there they passively collect live session tokens for every user whose session is created, changed, or ended — with no login attempts or lockouts triggered.

Why it matters

The record scores this 10.0 (CVSS 4.0). No login is needed, and the advisory says collection is passive — no failed logins, no lockouts — making active exposure hard to detect. The stolen token (iPlanetDirectoryPro value) is a bearer credential valid against OpenAM's REST endpoints and every application relying on OpenAM for SSO. The advisory says a captured administrator session gives an attacker full administrative capability and command execution as the OpenAM service account. Our reading is that the passive, credentialless nature of collection and the breadth of SSO impact make this worth acting on promptly even without a CISA listing.

What the vendor's advisory says

We read two pages on github.com and www.vulncheck.com. In short:

- The advisory (GHSA-5c3q-hp86-xjr8) says 16.1.4 fixes three weaknesses: the WebSocket auth bypass, session token broadcast to policy agents on session events, and an open redirect on the same legacy endpoints that appends session tokens to redirect URLs when cookie-less URL rewriting is enabled.
- The advisory says proof-of-concept code was withheld to give operators time to upgrade. No separate CVE identifiers are given for the companion weaknesses fixed in the same release.

Things people will get wrong

- Only internet-facing OpenAM deployments are at risk. The advisory says any attacker who can reach the OpenAM port is sufficient. An insider or a compromised system on the same internal segment has the same access as an external attacker.
- This is an information-disclosure flaw, not a takeover risk. The advisory says a captured administrator session gives full administrative capability and command execution on the server as the OpenAM service account, reached through the same REST endpoints.
- Disabling policy agent notifications is confirmed as a full workaround. The sources do not list any workaround. The advisory recommends upgrading to 16.1.4 and does not state that disabling agent notifications closes the exposure.

How we would triage it

This is our judgement.

Step 1: Find the OpenAM version installed

- Check the version banner in the OpenAM admin console, or look at the installed openam-server-only JAR filename in the web container's lib directory.
- The record says versions 14.0.0 through 16.1.3 are affected; 16.1.4 is the first unaffected version.

Step 2: Reduce network exposure while preparing to patch

- Restrict access to the OpenAM port to known-good clients using firewall rules or a network control while the upgrade is being planned.
- The advisory says the attacker needs only to reach the OpenAM port and hold a WebSocket connection; limiting who can reach that port limits the exposure without changing the application.

Step 3: Upgrade to OpenAM 16.1.4

- The vendor's advisory says 16.1.4 fixes all three weaknesses. Back up the OpenAM configuration store before starting the upgrade.
- Test in a non-production environment first if other applications depend on this OpenAM instance for single sign-on.

Step 4: Verify the upgrade is complete

- After the upgrade, confirm the running version is 16.1.4 by checking the admin console and the installed JAR filename using the same check as step one.
- Confirm that policy agents are reconnecting normally and that no session errors appear in the OpenAM logs.

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.

> *We are writing about CVE-2026-123551 affecting OpenIdentityPlatform OpenAM. Versions 14.0.0 through 16.1.3 contain a flaw that allows an unauthenticated attacker who can reach the OpenAM port to collect live session tokens passively, with no login required. The record scores this 10.0. The vendor's advisory (GHSA-5c3q-hp86-xjr8) says version 16.1.4 fixes the issue. Please confirm whether we run OpenAM and, if so, which version and on which systems. If we are on an affected version, please provide a written plan and date to upgrade to 16.1.4, and confirm in writing once the upgrade is complete.*

The weakness behind it

The record classes this as CWE-201.

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
Steal Web Session Cookie (T1539): Stealing a logged-in session cookie to act as that user without a password.	Credential Access: stealing logins	The flaw leaks iPlanetDirectoryPro session tokens over a WebSocket; passively collecting these would likely be used as stolen session credentials to impersonate any user.
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 attacker exploits an authentication bypass on a network-reachable WebSocket and legacy Liberty ID-FF endpoints, which would typically follow the pattern of exploiting a public-facing application.
Use Alternate Authentication Material (T1550): Using a stolen token or hash instead of a password to log in.	Defense Evasion: avoiding detection	Captured session tokens are bearer credentials valid directly against REST endpoints and SSO-integrated applications; an attacker would likely use them as alternate authentication material.

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

The CVE record:

> *OpenAM from 14.0.0 before 16.1.4 contains an information disclosure vulnerability that allows unauthenticated attackers to read live session tokens from the notification WebSocket. Attackers can bypass the agent-only check through an unvalidated internal forward on legacy Liberty ID-FF endpoints, collecting iPlanetDirectoryPro tokens to hijack user and administrator sessions.*

Versions of OpenIdentityPlatform OpenAM the record lists as affected:

- 14.0.0 up to, but not including, 16.1.4

It lists these as unaffected:

- 16.1.4

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-2026-123551
```

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-2026-123551
```

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 sources do not state whether disabling agent notifications or restricting the WebSocket endpoint is an accepted workaround in place of upgrading to 16.1.4.
- The sources do not say whether the legacy Liberty ID-FF endpoints involved in the bypass are present in all OpenAM deployments or only in those configured to use federation features.
- The sources do not confirm whether versions before 14.0.0 are affected or unaffected.
- The advisory says proof-of-concept code was withheld at publication time; the sources do not say whether it has since been released.
- Exploitation is not recorded. That is not the same as none.
- This is a new record: scores, versions and wording can change in the first days, and they are as at 8 November 2026. We read the vendor pages listed under Sources; nothing here has been tested.
- 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-2026-123551: score 10, `CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:H/VI:H/VA:H/SC:H/SI:H/SA:H` As the CVE record gives it.

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	None	No 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	High	Total loss of confidentiality.
Subsequent systems: integrity	High	Total loss of integrity.
Subsequent systems: availability	High	Total loss of availability.

Appendix 2. Timeline

Date	Event
8 November 2026	CVE record published by VulnCheck.

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
OpenAM 14.0.0 to 16.1.3 is reachable from the internet or an untrusted network segment.	High	This week, before 16.1.4 is in place.

OpenAM 14.0.0 to 16.1.3 is the SSO provider for multiple internal or external applications.	High	This week — a captured session reaches every integrated application.
OpenAM 14.0.0 to 16.1.3 is on an internal network reachable by all staff or contractor systems.	Medium	Next patch cycle; isolating the port reduces near-term risk.
OpenAM 14.0.0 to 16.1.3 is reachable only from a monitored management network with no untrusted access.	Low	Next scheduled maintenance window.
OpenAM is at 16.1.4 or later, or is not deployed in this environment.	None	None for this CVE.

Appendix 4. Definition of done

- Every OpenIdentityPlatform OpenAM you run is listed, with its version.
- Each is outside the affected list, or the vendor's fix or mitigation is in place.
- The version output or a screenshot is saved with the date.
- Anything not done has an owner and a date.

Sources

- CVE record for CVE-2026-123551: https://www.cve.org/CVERecord?id=CVE-2026-123551
- CISA Known Exploited Vulnerabilities catalogue: https://www.cisa.gov/known-exploited-vulnerabilities-catalog
- Advisory or release notes read: github.com/OpenIdentityPlatform/OpenAM/security/advisories: https://github.com/OpenIdentityPlatform/OpenAM/security/advisories/GHSA-5c3q-hp86-xjr8
- Advisory or release notes read: www.vulncheck.com/advisories/openam-14.0.0-before-16.1.4-session-: https://www.vulncheck.com/advisories/openam-14.0.0-before-16.1.4-session-token-disclosure-via-notification-websocket