contact@namiq.io · namiq.io

NamiQ

SECURITY ADVISORY

# SAP_SE SAP NetWeaver AS ABAP and ABAP Platform (SAML2 Service Provider): new CVE

**CVE-2026-120017 · record published 10 November 2026**

## Analysis Report

| | | | |
|---|---|---|---|
| PREPARED BY | NamiQ | DATE | 10 November 2026 |
| FACTS AS OF | 10 November 2026 | VERSION | 1.0 |
| SEVERITY | **Critical: CVSS 3.1 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/sap-se-sap-netweaver-as-abap-and-abap-cve-2026-120017

## The bottom line

> *Any organisation running SAP NetWeaver AS ABAP on SAP_BASIS 702 to 754 with the SAML2 Service Provider active must act without delay; the record scores this at 10. First, confirm whether SAML2 SP is enabled and restrict network access to the ABAP stack until SAP publishes a patch.*

## At a glance

| Fact | Detail |
|---|---|
| Product | SAP_SE SAP NetWeaver AS ABAP and ABAP Platform (SAML2 Service Provider) (CVE-2026-120017) |
| Severity | Critical: 10 (CVSS 3.1) |
| Status | A new CVE record, published by Sap on 10 November 2026. Not on CISA's list of exploited vulnerabilities when we read it on 10 November 2026, which means nothing public says yet that anyone is using it. |
| Fixed in | No source we read names a fixed version |
| Who looks first | Teams running SAP NetWeaver AS ABAP or the ABAP Platform on SAP_BASIS 702, 731, 740, 750, 751, 752, 753 or 754 where the SAML2 SP feature is configured. Systems unreachable by untrusted users over a network face lower immediate risk. |

## Does this apply to you?

**Answer in order. Stop at the first no.**

| Question | If no | If yes |
|---|---|---|
| Do you run SAP NetWeaver AS ABAP or the ABAP Platform? | Nothing to do for this CVE. | Check the BASIS version (next question). |
| Is your SAP_BASIS version 702, 731, 740, 750, 751, 752, 753 or 754? | Nothing to do for this CVE. | Check whether SAML2 Service Provider is active. |
| Is the SAML2 Service Provider feature enabled on this system? | SAML2 SP appears to be the trigger; keep it off and monitor SAP's notes. | Restrict network access and apply SAP's patch when published. |
| Can untrusted users send requests to the ABAP stack over the network? | Patch at the next cycle; watch for SAP's correction. | High priority: restrict access to the ABAP stack now. |

## What it is

The record says the ABAP platform does not properly verify incoming SAML authentication assertions under certain configurations. An unauthenticated attacker can send crafted assertions to bypass the login check and be recognised as any user, including system administrators, gaining full access to the application.

## Why it matters

A score of 10 means no credentials, no user interaction, and no prior foothold are needed. An attacker able to send an HTTP request to the ABAP stack can craft a SAML assertion and receive a session as any named account, including those with administrator rights, leading to the full compromise the record describes. CWE-347 covers failure to verify a cryptographic signature on a trusted assertion. The description says exploitation requires certain configurations, which the record does not define beyond naming the SAML2 SP component. Our reading is that systems where SAML2 SP is not active are likely unaffected, but the record does not confirm this, and the absence of any named fix makes verification essential.

## Things people will get wrong

- Our SAP is fully patched so we are safe The record lists no unaffected releases and no source names a fixed version. No available patch is confirmed to address this flaw; check SAP Security Notes directly for a specific correction.
- This only matters if SAP faces the internet An attacker already on the internal network who can send HTTP requests to the ABAP stack can exploit this bypass. Internal exposure is still exposure.

## How we would triage it

This is our judgement.

## Step 1: Find which SAP_BASIS versions you run

- On each SAP ABAP system, check the installed SAP_BASIS component level. The record lists SAP_BASIS 702, 731, 740, 750, 751, 752, 753 and 754 as affected ranges.
- Record the instance numbers and system IDs so you can track which systems need patching once SAP publishes a correction.

## Step 2: Confirm whether SAML2 Service Provider is active

- On each affected system, check whether the SAML2 SP feature is configured and in use. The record says exploitation requires certain configurations; the product name points to SAML2 SP as the trigger.
- If SAML2 SP is not active and you can confirm it has not been enabled, the system may not be exposed — but monitor SAP's notes for clarification.

## Step 3: Restrict network access to exposed ABAP stacks

- Where SAML2 SP is active and the system is reachable from untrusted networks, use network controls to limit which sources can reach the ICM HTTP and HTTPS ports until a patch is applied.
- SAP's patch day page states that SAP_BASIS Support Packages older than 24 months may not receive a fix; check whether your release is still in Mainstream or Extended Maintenance.

## Step 4: Apply SAP's patch when published

- No fixed version is named in the record. Monitor SAP Security Notes for a correction to this CVE and apply it to all affected systems; the source lists 10 November 2026 as a scheduled patch day.
- After patching, verify SAML2 SP authentication is working as expected and review access logs for any sessions that were created before the patch was in place.

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 have been alerted to CVE-2026-120017, a maximum-severity authentication-bypass flaw in SAP NetWeaver AS ABAP and the ABAP Platform (SAML2 Service Provider). The record scores it at 10 and states that an unauthenticated attacker can impersonate any user, including administrators, on affected systems. SAP_BASIS versions 702, 731, 740, 750, 751, 752, 753 and 754 are listed as affected; no fixed version has been confirmed yet. Please check: (1) whether we run any of these BASIS versions; (2) whether the SAML2 SP feature is active on those systems; and (3) what network controls currently limit access to the ABAP stack. We would like written confirmation of these findings and a plan to apply SAP's patch as soon as it is published.*

## The weakness behind it

The record classes this as CWE-347.

## 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 | SAP NetWeaver exposes HTTP/HTTPS interfaces over the network; crafting a SAML assertion to bypass authentication would likely target these network-accessible application endpoints directly. |
| 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 | Successful exploitation produces an authenticated session as any named account; an attacker would likely use this impersonated valid session to access resources and persist further. |
| Exploitation of Remote Services (T1210): Exploiting a flaw in a service on another machine to move to it. | Lateral Movement: moving to other machines | The record states that impact may extend to connected components and systems; this would typically involve exploiting remote services reachable from the compromised ABAP stack. |

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:

> *SAP NetWeaver AS ABAP and ABAP Platform does not perform sufficient verification of incoming authentication assertions under certain configurations. An unauthenticated attacker could submit specially crafted data to bypass authentication and impersonate arbitrary users, including privileged accounts. Successful exploitation could cause a full system compromise, with the impact potentially extending to connected components and systems beyond the affected system. This results in a high impact on confidentiality, integrity, and availability of the application.*

Versions of SAP_SE SAP NetWeaver AS ABAP and ABAP Platform (SAML2 Service Provider) the record lists as affected:

- SAP_BASIS 702
- SAP_BASIS 731
- SAP_BASIS 740
- SAP_BASIS 750
- SAP_BASIS 751
- SAP_BASIS 752
- SAP_BASIS 753
- SAP_BASIS 754

The record gives no version ranges. Use the vendor's advisory for the affected versions.

## 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-2026-120017
```

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-2026-120017
```

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

- No fixed version or unaffected SAP_BASIS level is named in the record; no source confirms when SAP will publish a correction for this CVE.
- The record says exploitation requires 'certain configurations' but does not define which options beyond the SAML2 SP component are relevant.
- Whether connected components and systems are reachable automatically on successful exploitation, or only after further attacker steps, is not stated in the record.
- Whether disabling the SAML2 SP feature fully removes exposure is not confirmed by the record or any named source.
- 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 10 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-2026-120017**: score 10, `CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A: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. |
| Privileges required | None | No account is needed. |
| User interaction | None | No one has to do anything. |
| Scope | Changed | Damage reaches beyond 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 |
|---|---|
| 10 November 2026 | CVE record published by Sap. |

## 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 |
|---|---|---|
| SAP ABAP stack with SAML2 SP enabled, reachable from an untrusted network or the internet | High | Immediately; isolate before patching |
| SAP ABAP stack on an affected BASIS version where SAML2 SP status is unknown | High | This week: confirm SAML2 SP status |
| SAP ABAP stack on an affected BASIS version, SAML2 SP active, internal access only | Medium | Within the patch cycle; monitor SAP notes |
| SAP ABAP stack on an affected BASIS version with SAML2 SP disabled | Low | Apply SAP's patch when available |

| | | |
|---|---|---|
| No SAP NetWeaver AS ABAP in the estate | None | None for this CVE |

## Appendix 4. Definition of done

- Every SAP_SE SAP NetWeaver AS ABAP and ABAP Platform (SAML2 Service Provider) 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-2026-120017: https://www.cve.org/CVERecord?id=CVE-2026-120017
- CISA Known Exploited Vulnerabilities catalogue: https://www.cisa.gov/known-exploited-vulnerabilities-catalog
- Advisory or release notes read: support.sap.com/en/my-support/knowledge-base/security-notes-new: https://support.sap.com/en/my-support/knowledge-base/security-notes-news.html?anchorId=section_370125364
- Reference in the CVE record: me.sap.com: https://me.sap.com/notes/3849308
- Reference in the CVE record: url.sap: https://url.sap/sapsecuritypatchday