contact@namiq.io · namiq.io

NamiQ

SECURITY ADVISORY

Microsoft Azure DevOps: new CVE

CVE-2026-109467 · record published 10 November 2026

Analysis Report

Teams that do not run Azure DevOps have nothing to do; everyone else should treat this as urgent — the record scores it 9.9 and no fixed version is yet named. Contact Microsoft for remediation …

PREPARED BY	NamiQ	DATE	11 November 2026
FACTS AS OF	11 November 2026	VERSION	1.0
SEVERITY	**Critical: CVSS 3.1 9.9**	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/microsoft-azure-devops-cve-2026-109467

The bottom line

> *Teams that do not run Azure DevOps have nothing to do; everyone else should treat this as urgent — the record scores it 9.9 and no fixed version is yet named. Contact Microsoft for remediation guidance immediately and restrict who can reach the service in the meantime.*

At a glance

Fact	Detail
Product	Microsoft Azure DevOps (CVE-2026-109467)
Severity	Critical: 9.9 (CVSS 3.1)
Status	A new CVE record, published by Microsoft on 10 November 2026. Not on CISA's list of exploited vulnerabilities when we read it on 11 November 2026, which means nothing public says yet that anyone is using it.
Fixed in	The record's affected ranges end before publication, Patch 9
Who looks first	Any team running Azure DevOps — self-hosted or cloud-connected — where the service is reachable over a network and at least one authorised account exists.

Does this apply to you?

Answer in order. Stop at the first no.

Question	If no	If yes
Do you run Azure DevOps anywhere in your environment?	Nothing to do for this CVE.	Check whether the instance is reachable over a network (next question).
Is your Azure DevOps instance reachable over a network — internal or internet?	Lower urgency; monitor for a patch from Microsoft.	Restrict access while awaiting a patch (next question).
Do any authorised user accounts exist with network access to the instance?	Risk is minimal; continue monitoring for a patch.	Treat as urgent; limit account access and apply the patch when available.

What it is

The record says Azure DevOps does not properly check authentication, allowing someone who already holds a valid account to send a request over the network and have Azure DevOps run code

on the system.

Why it matters

Our reading is that a score of 9.9 reflects the severity of network-reachable code execution. The record states the attacker must be 'authorised', meaning some form of valid account is required, but it does not say what privilege level is sufficient. CWE-287 (Improper Authentication) means the control that determines what an authenticated user may cause the system to execute has broken down. Code execution on a build and source-control platform would give an attacker reach into pipelines, stored secrets, and repositories. No vendor advisory was available when this note was written, so the scope and conditions are drawn from the record alone.

Things people will get wrong

- 'Authorised attacker' means only administrators can exploit this. The record says the attacker must be authorised but does not state the required privilege level. The record does not confirm that a low-privilege account is sufficient, nor that only high-privilege ones are.
- No fixed version listed means we can wait for the next scheduled update. The absence of a named fix means the exposure window is open-ended. The record was published 10 November 2026; contact Microsoft for current remediation guidance rather than waiting.

How we would triage it

This is our judgement.

Step 1: Confirm whether Azure DevOps is in your environment

- Check with your IT provider or asset inventory whether Azure DevOps is deployed — self-hosted, containerised, or as part of a managed Azure subscription.
- Note the installed version; the record lists all versions from 1.0.0 up to but not including the publication date of 10 November 2026 as affected.

Step 2: Reduce network exposure while no patch is available

- Restrict which accounts and IP ranges can reach the Azure DevOps service until a patch is available.
- The record names no workaround; reducing the pool of authorised users who can reach the service over a network lowers the attack surface.

Step 3: Apply the patch as soon as Microsoft releases it

- No fixed version is named in the record. Monitor Microsoft's release notes for Azure DevOps and apply any update that addresses CVE-2026-109467 as soon as it is published.
- A score of 9.9 warrants out-of-cycle patching; do not defer to the next scheduled maintenance window.

Step 4: Confirm the fix is in place

- After patching, verify that the installed version matches the release that addresses this CVE and that the service is running the updated build.
- Because no vendor advisory was available when this note was written, confirm the fixed version against Microsoft's release documentation once it is published.

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-2026-109467, a flaw in Microsoft Azure DevOps with a CVSS score of 9.9, published 10 November 2026. The record states that an authorised attacker can execute code over a network. We would like to know whether we run Azure DevOps anywhere in our environment, which version is installed, and whether Microsoft has released a patch. No fixed version was named in the record at the time of writing. Please confirm in writing which version is in use, whether it has been patched, and when the update was applied. We would like this confirmation by 17 November 2026.*

The weakness behind it

The record classes this as CWE-287.

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
Exploitation of Remote Services (T1210): Exploiting a flaw in a service on another machine to move to it.	Lateral Movement: moving to other machines	CWE-287 in a network-reachable service exploited by an already-authorised user would likely follow the pattern of exploiting a remote service to gain code execution beyond the account's normal scope.
Exploitation for Privilege Escalation (T1068): Using a flaw to gain higher rights than the account had, such as administrator or root.	Privilege Escalation: gaining higher rights	An authorised but limited account exploiting improper authentication to gain code execution would likely result in elevated privileges on the system running the service.

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:

> *Improper authentication in Azure DevOps allows an authorized attacker to execute code over a network.*

Versions of Microsoft Azure DevOps the record lists as affected:

- 1.0.0 up to, but not including, publication
- 1.0.0.0 up to, but not including, Patch 9

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-2026-109467
```

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-2026-109467
```

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 record does not name a fixed version; it is not known when Microsoft will release a patch for this flaw.
- The record does not say what privilege level an authorised attacker requires — whether a standard user account is sufficient or a higher role is needed.
- It is not known from the record whether the flaw affects cloud-hosted Azure DevOps Services, self-hosted Azure DevOps Server, or both.
- No workaround is recorded; it is not known whether disabling any specific feature or configuration reduces exposure.
- 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 11 November 2026. We have not read the vendor's advisory page and we have not tested it.
- 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-2026-109467: score 9.9, `CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:L/E:U/RL:O/RC:C` 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	Low	An ordinary account is enough.
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	Low	Reduced performance or interruptions.

Appendix 2. Timeline

Date	Event
10 November 2026	CVE record published by Microsoft.

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
Azure DevOps is internet-facing and has authorised user accounts	Medium	Immediately — restrict access; patch when available
Azure DevOps is on an internal network with authorised accounts	Medium	This week — patch when available; audit account access
Azure DevOps is running but no authorised accounts have network access	Low	Next patch cycle
Azure DevOps is not running in your environment	None	None for this CVE

Appendix 4. Definition of done

- Every Microsoft Azure DevOps 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-2026-109467: https://www.cve.org/CVERecord?id=CVE-2026-109467
- CISA Known Exploited Vulnerabilities catalogue: https://www.cisa.gov/known-exploited-vulnerabilities-catalog
- Reference in the CVE record: msrc.microsoft.com: https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-109467