contact@namiq.io · namiq.io

NamiQ

SECURITY ADVISORY

Microsoft Entra Device Registration: new CVE

CVE-2026-109469 · record published 6 November 2026

Analysis Report

Anyone running Microsoft Entra Device Registration must act: the record scores this 10 and requires no authentication. No fixed version is recorded; confirm whether this service is running and …

PREPARED BY	NamiQ	DATE	6 November 2026
FACTS AS OF	6 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/microsoft-entra-device-registration-cve-2026-109469

The bottom line

> *Anyone running Microsoft Entra Device Registration must act: the record scores this 10 and requires no authentication. No fixed version is recorded; confirm whether this service is running and reachable from untrusted networks, then watch for Microsoft guidance.*

At a glance

Fact	Detail
Product	Microsoft Entra Device Registration (CVE-2026-109469)
Severity	Critical: 10 (CVSS 3.1)
Status	A new CVE record, published by Microsoft on 6 November 2026. Not on CISA's list of exploited vulnerabilities when we read it on 6 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	Anyone running Microsoft Entra Device Registration, particularly where it is reachable from outside a trusted network. If your organisation uses Microsoft Entra for device management, check whether this component is active.

Does this apply to you?

Answer in order. Stop at the first no.

Question	If no	If yes
Do you use Microsoft Entra Device Registration?	Nothing to do for this CVE.	Continue to the next question.
Is Device Registration specifically enabled in your Entra configuration?	Nothing to do for this CVE unless you enable it later.	Continue to the next question.
Can anyone outside your trusted network reach the Device Registration service?	Lower urgency; apply any fix Microsoft publishes.	Treat as high priority; see steps below.

What it is

The flaw lets an attacker who can reach the service over a network bypass authorisation by substituting a key they control for one the system expects. No prior account or login is needed; the record says the attacker then elevates their privileges.

Things people will get wrong

- It is not on the CISA exploited list, so we can wait Absence from that list means exploitation has not been confirmed publicly, not that it is safe. A score of 10 warrants immediate attention; the record is newly published.
- Only attackers with an existing account can trigger this The record explicitly states 'unauthorized attacker', meaning no prior credentials are needed to reach or exploit the flaw over a network.

How we would triage it

This is our judgement.

Step 1: Confirm whether Entra Device Registration is in use

- Check the Microsoft Entra admin centre to confirm whether Device Registration is enabled and which networks or user groups can reach it.
- Note whether the service is accessible from outside your trusted network perimeter.

Step 2: Reduce network exposure while no fix is available

- If the service does not need to be reachable from untrusted networks, restrict access at the firewall or through Conditional Access policies in Entra.
- No source names a workaround that removes the flaw; restricting network reach limits who can attempt an exploit.

Step 3: Apply the Microsoft fix when published

- No fixed version is recorded as of 6 November 2026. Monitor Microsoft's security update guidance for CVE-2026-109469 and apply any patch promptly.
- No source names a workaround that fully removes the flaw.

Step 4: Confirm the update and check the configuration

- Once a fix is available and applied, confirm the updated version or policy state is in place before marking this resolved.
- Verify that Device Registration is accessible only from the networks and accounts that require it.

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 made aware of a critical vulnerability in Microsoft Entra Device Registration, reference CVE-2026-109469. The record scores it 10 and states that an unauthenticated attacker on the network can escalate privileges. No fixed version has been recorded as of 6 November 2026. We would like to know whether we run this service, which version or configuration is in place, whether it is reachable from outside our trusted network, and whether Microsoft has published guidance or a fix. Please provide written confirmation of the service status and your recommended next steps.*

The weakness behind it

The record classes this as CWE-639.

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 record describes a network-reachable flaw requiring no authentication; an attacker would likely exploit the registration service as a public-facing application to gain initial access or elevated privileges.

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	The description explicitly names privilege escalation as the outcome; CWE-639 would typically enable this by allowing an attacker to substitute their own key to claim elevated access.
Account Manipulation (T1098): Changing an existing account, for example adding permissions or keys, to keep access.	Persistence: staying in	The service manages device authorisation; a successful privilege escalation here would likely involve manipulating which devices or identities receive elevated standing, persisting as a trusted entity.

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:

> *Authorization bypass through user-controlled key in Entra Device Registration allows an unauthorized attacker to elevate privileges over a network.*

Versions of Microsoft Entra Device Registration the record lists as affected:

- -

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-2026-109469
```

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-2026-109469
```

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 expected patch date is recorded in the CVE record or any source that could be read.
- Whether the flaw affects cloud-hosted, hybrid, or on-premises Entra deployments is not stated in the record.
- Whether any configuration change or access restriction fully removes the attack surface while a patch is awaited is not recorded.
- 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 6 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", "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-2026-109469: score 10, `CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H/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	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
6 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
Entra Device Registration is active and reachable from the internet or an untrusted network	Medium	As soon as possible; apply any fix when Microsoft publishes one
Entra Device Registration is active but accessible only from your internal trusted network	Medium	This week; apply any fix when available
You use Microsoft Entra but are unsure whether Device Registration is enabled or who can reach it	Medium	Confirm this week; escalate to High if it proves externally reachable
You do not use Microsoft Entra Device Registration	None	None for this CVE

Appendix 4. Definition of done

- Every Microsoft Entra Device Registration 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-2026-109469: https://www.cve.org/CVERecord?id=CVE-2026-109469
- 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-2026-109469