contact@namiq.io · namiq.io

NamiQ

SECURITY ADVISORY

Zohocorp M365 Manager Plus: new CVE

CVE-2026-12591 · record published 12 November 2026

Analysis Report

If you run ManageEngine M365 Manager Plus, find your build and upgrade to 4818; builds 4817 and earlier are affected. It is not on CISA's list, and the flaw needs a logged-in technician account, so a …

PREPARED BY	NamiQ	DATE	12 November 2026
FACTS AS OF	12 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/zohocorp-m365-manager-plus-cve-2026-12591

The bottom line

> *If you run ManageEngine M365 Manager Plus, find your build and upgrade to 4818; builds 4817 and earlier are affected. It is not on CISA's list, and the flaw needs a logged-in technician account, so a server with no delegated technicians can wait for the next cycle.*

At a glance

Fact	Detail
Product	Zohocorp M365 Manager Plus (CVE-2026-12591)
Severity	Critical: 9.9 (CVSS 3.1)
Status	A new CVE record, published by Zohocorp on 12 November 2026. Not on CISA's list of exploited vulnerabilities when we read it on 12 November 2026, which means nothing public says yet that anyone is using it.
Fixed in	M365 Manager Plus build 4818 (the vendor's advisory says it was fixed on 24 June 2026; builds 4817 and earlier are affected).
Who looks first	Organisations running ManageEngine M365 Manager Plus, above all where day-to-day Microsoft 365 work is handed to technician accounts. Whoever looks after that server should check its build.

Does this apply to you?

Answer in order. Stop at the first no.

Question	If no	If yes
Do you run ManageEngine M365 Manager Plus?	Nothing to do for this CVE.	Check your build number (next question).
Is your build 4817 or earlier?	Build 4818 or later already has the fix.	Plan the upgrade to build 4818.
Do you grant delegated technician accounts in it?	Lower risk, but still upgrade.	Those accounts could escalate; upgrade.

What it is

The record says a logged-in technician can use weak permission checks in the delegated administration interface to gain rights beyond their intended role, which can lead to running code on the server during administrative processing.

Why it matters

The flaw needs an account, so it is not an open door for anonymous attackers; its value is to someone who already holds a limited technician login. The record says weak permission checks let that person step past their delegated scope and reach code execution during administrative processing. Our reading is that this can turn a low-trust helpdesk role into control of a server that holds broad Microsoft 365 administrative reach, so the risk grows with how widely you have delegated and how trusted those technicians are. The fix is a straightforward build upgrade.

What the vendor's advisory says

We read one page on www.manageengine.com. In short:

- The vendor's advisory rates this High and names builds 4817 and earlier as affected, with build 4818 as the fixed version.
- The advisory says the fix shipped on 24 June 2026 and does not list any other flaws fixed in the same build.

Things people will get wrong

- The score is 9.9, so anonymous attackers on the internet can walk straight in. The record says the attacker must first be an authenticated technician; the flaw is not reachable without an account.
- It needs no login, so it could spread on its own. The record describes an authenticated technician abusing weak permission checks, not an unauthenticated path.

The wording includes conditions the score may not show: authenticated. Read the record before you decide it does not apply to you.

How we would triage it

This is our judgement.

Step 1: Find the builds you run

- Check the build number of each M365 Manager Plus install. Builds 4817 and earlier are affected; build 4818 holds the fix.

Step 2: Review who holds technician delegation

- List the technician accounts with delegated administration rights and remove any that are not needed, because only a logged-in technician can use this flaw.

Step 3: Upgrade to the fixed build

- Upgrade to build 4818. The vendor's advisory says this build fixes the flaw and was released on 24 June 2026.

Step 4: Confirm the fix is in place

- After upgrading, confirm the build reads 4818 or later, and keep a record of which accounts hold technician delegation.

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 checking our exposure to CVE-2026-12591 in ManageEngine M365 Manager Plus. Could you confirm in writing whether we run it, on which server, and the exact build number? The vendor's advisory says builds 4817 and earlier are affected and build 4818 fixes it, released on 24 June 2026. The flaw lets a logged-in technician escalate beyond their delegated scope to code execution, so please also tell us which accounts hold delegated administration rights. Please confirm the current build and that the upgrade to 4818 is in place by a date we agree.*

The weakness behind it

The record classes this as CWE-862.

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
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	The record says the attacker must be an authenticated technician, so a valid, if limited, account would likely be the starting point.
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 record describes escalating privileges beyond the intended scope by exploiting weak permission checks, which this technique would typically cover.

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:

> *Zohocorp ManageEngine M365 Manager Plus versions below 4818 is affected by an authenticated technician may exploit insufficient permission validation in the delegated administration interface to escalate privileges beyond their intended scope, which could result in remote code execution during administrative processing.*

Versions of Zohocorp M365 Manager Plus the record lists as affected:

- all versions before 4818

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-2026-12591
```

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-2026-12591
```

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 say whether this flaw has been used against anyone.
- They do not give a workaround for those who cannot upgrade to 4818 straight away.
- They do not say which technician privileges are enough to trigger it.
- They do not say whether lower-privileged accounts can reach the delegated administration interface.
- 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 12 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-2026-12591: score 9.9, `CVSS:3.1/AV:N/AC:L/PR:L/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	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	High	Total loss of availability.

Appendix 2. Timeline

Date	Event
12 November 2026	CVE record published by Zohocorp.

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
An M365 Manager Plus server with many delegated technician accounts	Medium	this patch cycle
An M365 Manager Plus server any logged-in technician can reach	Medium	this week
A server on build 4817 or earlier with few, trusted operators	Low	next patch cycle
No M365 Manager Plus anywhere in the estate	None	none for this CVE

Appendix 4. Definition of done

- Every Zohocorp M365 Manager Plus 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-2026-12591: https://www.cve.org/CVERecord?id=CVE-2026-12591
- CISA Known Exploited Vulnerabilities catalogue: https://www.cisa.gov/known-exploited-vulnerabilities-catalog
- Advisory or release notes read: www.manageengine.com/microsoft-365-management-reporting/CVE-2026-125: https://www.manageengine.com/microsoft-365-management-reporting/CVE-2026-12591.html