contact@namiq.io · namiq.io

NamiQ

SECURITY ADVISORY

Microsoft Office exploited

CVE-2026-124194 · on CISA's exploited list since 10 November 2026

Analysis Report

Anyone running Outlook from Microsoft 365 Apps, Office LTSC 2021 or 2024 should plan to patch before 24 November 2026. First, find which Office build each machine runs and compare it with the fixed ...

PREPARED BY	NamiQ	DATE	13 November 2026
FACTS AS OF	13 November 2026	VERSION	1.0
SEVERITY	**Medium: CVSS 3.1 6.5**	STATUS	On CISA's exploited list; due 24 November 2026

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-office-cve-2026-124194

The bottom line

> *Anyone running Outlook from Microsoft 365 Apps, Office LTSC 2021 or 2024 should plan to patch before 24 November 2026. First, find which Office build each machine runs and compare it with the fixed builds below.*

At a glance

Fact	Detail
Product	Microsoft Office (CVE-2026-124194)
Severity	Medium: 6.5 (CVSS 3.1)
CISA	On its exploited list since 10 November 2026. Deadline for US federal agencies: 24 November 2026.
Chance of exploitation (EPSS)	0.02, the estimated chance in the next 30 days, as at 13 November 2026
Ransomware use	Not recorded by CISA. That is not the same as none.
Fixed in	Office LTSC 2021: 16.0.14334.21048. Office LTSC 2024: 16.0.17932.21140. Microsoft 365 Apps for Enterprise: the record names no version, only a vendor releases page.
Who looks first	Anyone running Outlook from Microsoft 365 Apps for Enterprise, Office LTSC 2021 or Office LTSC 2024.

Does this apply to you?

Answer in order. Stop at the first no.

Question	If no	If yes
Do you run Outlook from Microsoft 365 Apps, Office LTSC 2021 or Office LTSC 2024?	Nothing to do for this CVE.	Check the build you run next.
Is your Office build below the fixed build listed above?	You are already on a fixed build.	Plan the update.
Do your users open mail from outside your organisation?	Lower urgency, still patch.	Treat as higher priority; a user action triggers it.

What it is

The record says Outlook does not warn the user before a potentially unsafe action. An attacker with no login can craft a message that spoofs over a network, but the user still has to click or open something for it to work.

Why it matters

The flaw needs the user to click or open something, so it is not a silent remote break-in. Its value to an attacker is deception: the record says Outlook does not warn before a potentially unsafe action, so a message can be dressed up to look trustworthy. Our reading is that it fits alongside phishing, because the missing warning removes the moment a careful user would otherwise pause. The score is middling, but the low bar, no attacker login and just a convincing message, is why it is worth clearing promptly.

Things people will get wrong

- We use webmail or browser Outlook, so this does not apply. The record lists desktop products: Microsoft 365 Apps for Enterprise, Office LTSC 2021 and 2024. Confirm which Outlook you run before deciding.
- It is only spoofing, so it is harmless. The record says the user is not warned of an unsafe action. Spoofing here means a message can be made to look trustworthy, which is useful for getting a person to act.

The wording includes conditions the score may not show: someone must click or open something. 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 Office build you run

- Check each machine's Office product and build number against the affected ranges. The record lists Microsoft 365 Apps for Enterprise, Office LTSC 2021 and Office LTSC 2024.

Step 2: Reduce exposure while you wait

- Remind users not to act on unexpected prompts in mail, especially from outside senders. The flaw needs someone to click or open something, so user caution lowers the risk until the update lands.

Step 3: Update to the fixed build

- For Office LTSC 2021 move to 16.0.14334.21048 or later, and for Office LTSC 2024 to 16.0.17932.21140 or later. For Microsoft 365 Apps for Enterprise follow the vendor's releases, as the record names no single fixed number.

Step 4: Confirm the build after updating

- Re-check the build number on each machine to confirm it is at or above the fixed build for that product.

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. CISA's wording adds that you should stop using the product if no mitigation is available.

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 following up on a security issue in Microsoft Outlook, CVE-2026-124194. Could you tell us whether we run Outlook from Microsoft 365 Apps for Enterprise, Office LTSC 2021 or Office LTSC 2024, on which machines, and which build each is on? The fixed builds are 16.0.14334.21048 for Office LTSC 2021 and 16.0.17932.21140 for Office LTSC 2024; for Microsoft 365 Apps the record points to the vendor's releases rather than a single number. CISA has set 24 November 2026 for applying the vendor's mitigations. Please confirm in writing the build we run and that the fix is in place by 21 November 2026. Thank you.*

Signs it was used

An update closes the hole. It does not tell you whether someone used it first. CISA's required action points to its forensic triage requirements (BOD 26-04). Look for:

- Mail that prompted a user to take an action without the usual warning, especially from external senders.

The weakness behind it

The record classes this as CWE-356 (Missing User Interaction for Potentially Unsafe Action).

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
Phishing (T1566): Sending a message, usually email, that tricks someone into opening a file or link.	Initial Access: getting in	The record says the user is not warned of an unsafe action and must click or open something. An attacker would likely deliver a crafted message, so this initial-access route fits.
User Execution (T1204): Relying on a person to run a file or open a link.	Execution: running the attacker's code	The record says someone must click or open something for the spoofing to work, so success would typically rely on the user acting on the attacker's content.

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

CISA's catalogue entry:

> *Microsoft Office Outlook contains a missing user interaction for potentially unsafe action vulnerability that allows an unauthorized attacker to perform spoofing over a network.*

The CVE record, published by Microsoft on 10 November 2026:

> *Product ui does not warn user of unsafe actions in Microsoft Office Outlook allows an unauthorized attacker to perform spoofing over a network.*

Versions of Microsoft 365 Apps for Enterprise the record lists as affected:

- 16.0.1 up to, but not including, https://aka.ms/OfficeSecurityReleases

The affected ranges end before https://aka.ms/OfficeSecurityReleases. Those are the first versions the record does not list as affected; confirm them in the vendor's advisory.

Versions of Microsoft Office LTSC 2021 the record lists as affected:

- 16.0.1 up to, but not including, 16.0.14334.21048

The affected ranges end before 16.0.14334.21048. Those are the first versions the record does not list as affected; confirm them in the vendor's advisory.

Versions of Microsoft Office LTSC 2024 the record lists as affected:

- 16.0.0 up to, but not including, 16.0.17932.21140

The affected ranges end before 16.0.17932.21140. Those are the first versions the record does not list as affected; confirm them in the vendor's advisory.

CISA's required action:

> *Apply mitigations in accordance with vendor instructions.*

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-2026-124194
```

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-2026-124194
```

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 single fixed build for Microsoft 365 Apps for Enterprise; it points to the vendor's releases rather than a version number.
- It does not say whether previewing a message in the reading pane triggers the flaw, or only fully opening it.
- It does not describe what the unsafe action is that the user is not warned about.
- It does not say whether Outlook on macOS or the web, if any, is affected.
- We have not tested this against any environment. Versions and scores are as the sources state them and as at 13 November 2026; the vendor's advisory wins where it differs.
- 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-2026-124194: score 6.5, `CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:N/A:N/E:H/RL:O/RC:C` As the CVE record gives it. The record's own score can differ from the base score on the NVD record.

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	Required	A person must click, visit or open something.
Scope	Unchanged	Damage stays inside the vulnerable component.
Confidentiality	High	Total loss of confidentiality.
Integrity	None	Nothing can be altered.
Availability	None	No effect on availability.

Appendix 2. Timeline

Date	Event
10 November 2026	CVE record published by Microsoft.
10 November 2026	CISA added it to its list of exploited vulnerabilities.
24 November 2026	CISA's deadline for US federal agencies.

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
Outlook on an affected build, users regularly open mail from outside the organisation	High	within CISA's window
Microsoft 365 Apps for Enterprise, build not yet confirmed	Medium	this week
Affected build, but mail is tightly filtered with few external senders	Medium	this week
Office LTSC 2021 or 2024 already at or above the fixed build	None	none for this CVE

Appendix 4. Definition of done

- Every Microsoft Office you run is listed, with its version.
- Each is outside the affected list, or the vendor's mitigation is in place.
- The version output or a screenshot is saved with the date.
- Your projects' declared dependencies were checked against this CVE, and every row has a written reason.
- Logs for the weeks before the update were searched, and anything odd was written down.
- Anything not done has an owner and a date.

Sources

- CISA Known Exploited Vulnerabilities catalogue: https://www.cisa.gov/known-exploited-vulnerabilities-catalog
- CVE record for CVE-2026-124194: https://www.cve.org/CVERecord?id=CVE-2026-124194
- FIRST: Exploit Prediction Scoring System: https://www.first.org/epss/
- Reference in the CVE record: msrc.microsoft.com: https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-124194