SERVICE ALERT

Prepared Nov 13, 2026, 1:31 PM PST

Microsoft CVE- MS CVE-2026-124194

Status: Recovering / monitoring

Started Nov 10, 2026, 12:00 AM PST · Ongoing for 3 days 13 hours · Microsoft's estimate: Fix already released with Microsoft's November 10, 2026 update; deployment is up to each customer.

MICROSOFT REFERENCE NUMBERS

CVE-2026-124194 EUVD-2026-122310

Quote these to Microsoft or to BIS support.

SUMMARY

Microsoft has fixed an actively exploited flaw in classic Outlook for Windows (CVE-2026-124194) that could expose a user's Windows login hash when a crafted email file is opened. The fix is in Microsoft's November 10, 2026 Office update, not Windows Update, so we are installing it on affected machines and will confirm when done. This is separate from the November 12 Microsoft 365 outage, which Microsoft has not linked to this flaw.

Affected: Outlook for Windows (classic), Microsoft 365 Apps for Enterprise, Office LTSC 2021, Office LTSC 2024

LATEST NEWS

Microsoft fixed CVE-2026-124194, an actively exploited Outlook spoofing flaw, in its November 10, 2026 Office security updates. Secondary reports say Windows Update does not deliver the fix, and Microsoft has not linked it to the November 12 Microsoft 365 outage.

Microsoft says (Nov 10, 2026, 12:00 AM PST): “Microsoft's advisory describes a spoofing flaw in Outlook where the product UI does not warn users of unsafe actions, allowing an unauthenticated attacker to spoof over a network with user interaction; it is marked exploited.”

Source: https://msrc.microsoft.com/update-guide/advisory/CVE-2026-124194

IS THIS A HACK?

Yes — the vendor or a reliable source has confirmed an attack or active exploitation.

Microsoft and CISA list the flaw as exploited, so it is being used in real attacks; a victim must open a crafted message file.

ROOT CAUSE

Outlook does not show the external-content warning before connecting to an attacker-controlled network location, which can leak the user's NTLMv2 hash.

WHAT THE IT COMMUNITY IS SAYING

The posts I could find this round about CVE-2026-124194 were mostly on X, which is not an allowed source, so I left them out. The allowed-site hits were LinkedIn profile pages that repeat the points that a crafted message file leaks an NTLMv2 hash, that CISA lists the flaw as exploited with a November 24 federal deadline, and that the fix ships in Office updates rather than Windows Update. No Reddit or Bluesky thread on this CVE surfaced, and nobody on an allowed site reported a failed fix, a confirmed fix on their own machines, or a public exploit.

From public posts by IT administrators; not confirmed by the vendor.

LAST 4 UPDATES

Nov 13, 2026, 7:16 AM PST

New: SecurityWeek reports Microsoft has not linked the flaw to the November 12 Microsoft 365 outage; a secondary guide lists a Microsoft 365 Apps build, and Splashtop says the Windows cumulative update does not carry the fix. None are confirmed by Microsoft.

Questions? Contact BIS Computer Solutions, Inc.

Phone: +1-818-248-5023 · Fax: +1-818-249-1169 · Email: support@biscomputer.com · Web: www.biscomputer.com

Nov 12, 2026, 10:24 PM PST

New since the last check: a CVE mirror now shows NVD as "Analyzed", CISA's catalog gives the official vulnerability name and says ransomware use is unknown, and one aggregator claims a public exploit exists, which conflicts with Microsoft.

Nov 12, 2026, 7:26 PM PST

Nothing major is new: a European exploitation listing (ENISA EUVD) and a Microsoft 365 Apps build-data gap, plus a conflicting CVSS score in one secondary source.

Nov 12, 2026, 4:08 PM PST

New details since the last check: the CVE record's CVSS vector marks exploit maturity as High, 64-bit Office editions are listed as affected, Microsoft's exploited flag is paired with "not publicly disclosed," and a second public PoC repository is listed.