



NCSC-2026-0058

Kwetsbaarheden verholpen in Microsoft Office

NCSC Advisory

Prioriteit: Normaal

Gepubliceerd op: 10-02-2026

TLP:WHITE

Toegestane verspreiding van TLP:WHITE

(Traffic Light Protocol)

Deze handreiking bevat het label TLP:WHITE en wordt door het NCSC verspreid. Het NCSC gebruikt het Traffic Light Protocol (TLP) om eenduidig te definiëren wat er met de informatie mag gebeuren. Wanneer informatie is voorzien van een TLP-aanduiding weet u met wie u deze informatie mag delen. Dit staat beschreven in de standaard First (www.first.org/tlp).

Ontvangers van TLP:WHITE mogen de informatie publiek verspreiden.

Uw reacties zijn welkom op info@ncsc.nl

Feiten

Microsoft heeft kwetsbaarheden verholpen in Office componenten.

Duiding

Een kwaadwillende kan de kwetsbaarheden misbruiken om beveiligingsmaatregelen te omzeilen, zich voor te doen als andere gebruiker en zich zo verhoogde rechten toe te kennen en toegang te krijgen tot gevoelige gegevens.

Voor succesvol misbruik moet de kwaadwillende het slachtoffer misleiden en malafide bestand te openen of link te volgen.

Van de kwetsbaarheid met kenmerk CVE-2026-21511 meldt Microsoft informatie te hebben dat deze besproken wordt op fora. De kwetsbaarheid stelt een kwaadwillende in staat om middels een malafide bericht een NTLM-authenticatie te initiëren naar een server onder controle van de kwaadwillende, waarmee de kwaadwillende authenticatiegegevens kan bemachtigen. Er is (nog) geen publieke Proof-of-Concept-code beschikbaar en misbruik vereist een speciaal ingerichte server. Grootschalig misbruik is hiermee niet waarschijnlijk.

Microsoft Office Word:

CVE-ID	CVSS	Impact
CVE-2026-21514	7.80	Omzeilen van beveiligingsmaatregel

Microsoft Office Excel:

CVE-ID	CVSS	Impact
CVE-2026-21259	7.30	Verkrijgen van verhoogde rechten
CVE-2026-21258	5.50	Toegang tot gevoelige gegevens
CVE-2026-21261	5.50	Toegang tot gevoelige gegevens

Microsoft Office Outlook:

CVE-ID	CVSS	Impact
CVE-2026-21260	7.50	Voordoen als andere gebruiker
CVE-2026-21511	7.50	Voordoen als andere gebruiker

Oplossingen

Microsoft heeft updates beschikbaar gesteld waarmee de beschreven kwetsbaarheden worden verholpen. We raden u aan om deze updates te installeren. Meer informatie over de kwetsbaarheden, de installatie van de updates en eventuele work-arounds vindt u op:

<https://portal.msrc.microsoft.com/en-us/security-guidance>

Kwetsbaarheden

CVE	CVSS Score
> CVE-2026-21259	7.8 HIGH
> CVE-2026-21258	5.5 MEDIUM
> CVE-2026-21261	5.5 MEDIUM
> CVE-2026-21260	7.5 HIGH
> CVE-2026-21511	7.5 HIGH
> CVE-2026-21514	7.8 HIGH

CWE's

CWE	Beschrijving
> CWE-20	Improper Input Validation
> CWE-122	Heap-based Buffer Overflow
> CWE-125	Out-of-bounds Read
> CWE-200	Exposure of Sensitive Information to an Unauthorized Actor
> CWE-502	Deserialization of Untrusted Data
> CWE-807	Reliance on Untrusted Inputs in a Security Decision

Getroffen producten

Microsoft
Microsoft 365 Apps for Enterprise
Microsoft 365 Apps for Enterprise for 32-bit Systems
Microsoft 365 Apps for Enterprise for 64-bit Systems
Microsoft Excel 2016
Microsoft Excel 2016 (32-bit edition)
Microsoft Excel 2016 (64-bit edition)
Microsoft Office 2019
Microsoft Office 2019 for 32-bit editions
Microsoft Office 2019 for 64-bit editions
Microsoft Office LTSC 2021
Microsoft Office LTSC 2021 for 32-bit editions
Microsoft Office LTSC 2021 for 64-bit editions
Microsoft Office LTSC 2024
Microsoft Office LTSC 2024 for 32-bit editions

Microsoft Office LTSC 2024 for 64-bit editions
Microsoft Office LTSC for Mac 2021
Microsoft Office LTSC for Mac 2024
Microsoft Outlook 2016
Microsoft Outlook 2016 (32- bit edition)
Microsoft Outlook 2016 (64- bit edition)
Microsoft SharePoint Enterprise Server 2016
Microsoft SharePoint Server 2019
Microsoft SharePoint Server Subscription Edition
Microsoft Word 2016
Microsoft Word 2016 (32- bit edition)

Disclaimer

The Netherlands Cyber Security Center (henceforth: NCSC-NL) maintains this page to enhance access to its information and security advisories. The use of this security advisory is subject to the following terms and conditions: NCSC-NL makes every reasonable effort to ensure that the content of this page is kept up to date, and that it is accurate and complete. Nevertheless, NCSC-NL cannot entirely rule out the possibility of errors, and therefore cannot give any warranty in respect of its completeness, accuracy or continuous keeping up-to-date. The information contained in this security advisory is intended solely for the purpose of providing general information to professional users. No rights can be derived from the information provided therein. NCSC-NL and the Kingdom of the Netherlands assume no legal liability or responsibility for any damage resulting from either the use or inability of use of this security advisory. This includes damage resulting from the inaccuracy of incompleteness of the information contained in the advisory. This security advisory is subject to Dutch law. All disputes related to or arising from the use of this advisory will be submitted to the competent court in The Hague. This choice of means also applies to the court in summary proceedings.