



NCSC-2026-0116

Kwetsbaarheden verholpen in Microsoft Office

NCSC Advisory

Prioriteit: Normaal

Gepubliceerd op: 14-04-2026

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 diverse Office producten.

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.

Microsoft Office PowerPoint:

| CVE-ID | CVSS | Impact |
|----------------|------|---------------------------------|
| CVE-2026-32200 | 7,80 | Uitvoeren van willekeurige code |

Microsoft Office Word:

| CVE-ID | CVSS | Impact |
|----------------|------|---------------------------------|
| CVE-2026-33095 | 7,80 | Uitvoeren van willekeurige code |
| CVE-2026-33822 | 6,10 | Toegang tot gevoelige gegevens |
| CVE-2026-23657 | 7,80 | Uitvoeren van willekeurige code |
| CVE-2026-33114 | 8,40 | Uitvoeren van willekeurige code |
| CVE-2026-33115 | 8,40 | Uitvoeren van willekeurige code |

Microsoft Office:

| CVE-ID | CVSS | Impact |
|----------------|------|---------------------------------|
| CVE-2026-32190 | 8,40 | Uitvoeren van willekeurige code |

Microsoft Office SharePoint:

| CVE-ID | CVSS | Impact |
|--------|------|--------|
|--------|------|--------|

| | | |
|----------------|------|-------------------------------|
| CVE-2026-20945 | 4,60 | Voordoen als andere gebruiker |
| CVE-2026-32201 | 6,50 | Voordoen als andere gebruiker |

Microsoft Office Excel:

| CVE-ID | CVSS | Impact |
|----------------|------|---------------------------------|
| CVE-2026-32188 | 7,10 | Toegang tot gevoelige gegevens |
| CVE-2026-32189 | 7,80 | Uitvoeren van willekeurige code |
| CVE-2026-32197 | 7,80 | Uitvoeren van willekeurige code |
| CVE-2026-32198 | 7,80 | Uitvoeren van willekeurige code |
| CVE-2026-32199 | 7,80 | Uitvoeren van willekeurige code |

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-2026-20945 | 4.6 MEDIUM |
| > CVE-2026-23657 | 7.8 HIGH |
| > CVE-2026-32188 | 7.1 HIGH |
| > CVE-2026-32189 | 7.8 HIGH |
| > CVE-2026-32190 | 8.4 HIGH |
| > CVE-2026-32197 | 7.8 HIGH |
| > CVE-2026-32198 | 7.8 HIGH |

| | |
|------------------|------------|
| > CVE-2026-32199 | 7.8 HIGH |
| > CVE-2026-32200 | 7.8 HIGH |
| > CVE-2026-32201 | 6.5 MEDIUM |
| > CVE-2026-33095 | 7.8 HIGH |
| > CVE-2026-33114 | 8.4 HIGH |
| > CVE-2026-33115 | 8.4 HIGH |
| > CVE-2026-33822 | 6.1 MEDIUM |

CWE's

| CWE | Beschrijving |
|-----------|--|
| > CVE-20 | Improper Input Validation |
| > CVE-79 | Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') |
| > CVE-125 | Out-of-bounds Read |
| > CVE-416 | Use After Free |
| > CVE-822 | Untrusted Pointer Dereference |

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 2016 |
| Microsoft Office 2016 (32-bit edition) |
| Microsoft Office 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 PowerPoint 2016 |
| Microsoft PowerPoint 2016 (32-bit edition) |
| Microsoft PowerPoint 2016 (64-bit edition) |
| Microsoft SharePoint Enterprise Server 2016 |
| Microsoft SharePoint Server 2019 |
| Microsoft SharePoint Server Subscription Edition |
| Office Online Server |
| SharePoint Server |

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.