Nationaal Cyber Security Centrum
Ministerie van Justitie en Veiligheid

NCSC-2026-0182

Kwetsbaarheden verholpen in Microsoft Office

NCSC Security Advisory
Prioriteit: Normaal
Gepubliceerd op: 09-06-2026

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 als Sharepoint, Wordt, Project en Excel.

Duiding

Een kwaadwillende kan de kwetsbaarheden misbruiken om aanvallen uit te voeren die kunnen leiden tot de categorieën schade, zoals omschreven in onderstaande tabellen.

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

Microsoft Office SharePoint:

CVE-ID	CVSS	Impact
CVE-2026-45467	4.60	Voordoen als andere gebruiker
CVE-2026-45468	4.60	Voordoen als andere gebruiker
CVE-2026-45479	4.60	Voordoen als andere gebruiker
CVE-2026-45453	5.40	Voordoen als andere gebruiker
CVE-2026-47298	8.00	Uitvoeren van willekeurige code
CVE-2026-47636	5.40	Voordoen als andere gebruiker
CVE-2026-47637	4.60	Voordoen als andere gebruiker
CVE-2026-47638	4.60	Voordoen als andere gebruiker
CVE-2026-47639	5.40	Voordoen als andere gebruiker
CVE-2026-47641	4.60	Voordoen als andere gebruiker
CVE-2026-33113	5.40	Voordoen als andere gebruiker
CVE-2026-45454	6.50	Uitvoeren van willekeurige code
CVE-2026-45462	4.60	Voordoen als andere gebruiker
CVE-2026-45464	5.40	Voordoen als andere gebruiker
CVE-2026-45465	5.40	Voordoen als andere gebruiker
CVE-2026-47634	7.30	Voordoen als andere gebruiker
CVE-2026-47640	4.60	Voordoen als andere gebruiker
CVE-2026-45481	7.30	Voordoen als andere gebruiker
CVE-2026-45484	8.80	Verkrijgen van verhoogde rechten
CVE-2026-48560	5.40	Voordoen als andere gebruiker
CVE-2026-48562	4.60	Voordoen als andere gebruiker

Windows Win32K - GRFX:

|---|---|---|

CVE-ID	CVSS	Impact
CVE-2026-44803	7.80	Uitvoeren van willekeurige code
CVE-2026-44812	7.80	Uitvoeren van willekeurige code

Microsoft Office Word:

CVE-ID	CVSS	Impact
CVE-2026-45475	7.80	Uitvoeren van willekeurige code
CVE-2026-45471	7.80	Uitvoeren van willekeurige code
CVE-2026-45486	7.80	Uitvoeren van willekeurige code
CVE-2026-45485	3.30	Toegang tot gevoelige gegevens
CVE-2026-44819	7.80	Uitvoeren van willekeurige code
CVE-2026-44821	5.50	Toegang tot gevoelige gegevens
CVE-2026-44824	7.80	Uitvoeren van willekeurige code
CVE-2026-45466	3.30	Toegang tot gevoelige gegevens
CVE-2026-45643	7.80	Uitvoeren van willekeurige code
CVE-2026-45457	7.80	Uitvoeren van willekeurige code

Microsoft Teams for Android:

CVE-ID	CVSS	Impact
CVE-2026-42835	8.10	Toegang tot gevoelige gegevens

Office for Android:

CVE-ID	CVSS	Impact
CVE-2026-45649	7.10	Voordoen als andere gebruiker

Microsoft Office Project:

CVE-ID	CVSS	Impact
CVE-2026-45483	4.60	Voordoen als andere gebruiker

|----------------|------|-------------------------------------|

Microsoft Office:

CVE-ID	CVSS	Impact
CVE-2026-45472	8.40	Uitvoeren van willekeurige code
CVE-2026-45474	8.40	Uitvoeren van willekeurige code
CVE-2026-45456	8.40	Uitvoeren van willekeurige code
CVE-2026-45458	8.40	Uitvoeren van willekeurige code
CVE-2026-45460	4.70	Toegang tot gevoelige gegevens
CVE-2026-45461	8.40	Uitvoeren van willekeurige code
CVE-2026-45645	7.80	Uitvoeren van willekeurige code
CVE-2026-47635	8.40	Uitvoeren van willekeurige code
CVE-2026-45463	8.40	Uitvoeren van willekeurige code

Microsoft Office Excel:

CVE-ID	CVSS	Impact
CVE-2026-45469	7.80	Uitvoeren van willekeurige code
CVE-2026-44817	7.80	Uitvoeren van willekeurige code
CVE-2026-44818	7.00	Uitvoeren van willekeurige code
CVE-2026-44820	7.80	Uitvoeren van willekeurige code
CVE-2026-44823	7.80	Uitvoeren van willekeurige code
CVE-2026-44822	8.20	Toegang tot gevoelige gegevens
CVE-2026-45455	3.30	Toegang tot gevoelige gegevens
CVE-2026-45459	3.30	Omzeilen van beveiligingsmaatregel

Microsoft Office Click-To-Run:

CVE-ID	CVSS	Impact
CVE-2026-47293	7.00	Verkrijgen van verhoogde rechten

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-2026-33113	5.4 MEDIUM
CVE-2026-42835	8.1 HIGH
CVE-2026-44803	7.8 HIGH
CVE-2026-44812	7.8 HIGH
CVE-2026-44817	7.8 HIGH
CVE-2026-44818	7.0 HIGH
CVE-2026-44819	7.8 HIGH
CVE-2026-44820	7.8 HIGH
CVE-2026-44821	5.5 MEDIUM
CVE-2026-44822	8.2 HIGH
CVE-2026-44823	7.8 HIGH
CVE-2026-44824	7.8 HIGH
CVE-2026-45453	5.4 MEDIUM
CVE-2026-45454	6.5 MEDIUM
CVE-2026-45455	3.3 LOW
CVE-2026-45456	8.4 HIGH

CVE-2026-45457	7.8 HIGH
CVE-2026-45458	8.4 HIGH
CVE-2026-45459	3.3 LOW
CVE-2026-45460	4.7 MEDIUM
CVE-2026-45461	8.4 HIGH
CVE-2026-45462	4.6 MEDIUM
CVE-2026-45463	8.4 HIGH
CVE-2026-45464	5.4 MEDIUM
CVE-2026-45465	5.4 MEDIUM
CVE-2026-45466	3.3 LOW
CVE-2026-45467	4.6 MEDIUM
CVE-2026-45468	4.6 MEDIUM
CVE-2026-45469	7.8 HIGH
CVE-2026-45471	7.8 HIGH
CVE-2026-45472	8.4 HIGH
CVE-2026-45474	8.4 HIGH
CVE-2026-45475	7.8 HIGH
CVE-2026-45479	4.6 MEDIUM
CVE-2026-45481	7.3 HIGH
CVE-2026-45483	4.6 MEDIUM
CVE-2026-45484	8.8 HIGH
CVE-2026-45485	3.3 LOW
CVE-2026-45486	7.8 HIGH

CVE-2026-45643	7.8 HIGH
CVE-2026-45645	7.8 HIGH
CVE-2026-45649	7.1 HIGH
CVE-2026-47293	7.0 HIGH
CVE-2026-47298	8.0 HIGH
CVE-2026-47634	7.3 HIGH
CVE-2026-47635	8.4 HIGH
CVE-2026-47636	5.4 MEDIUM
CVE-2026-47637	4.6 MEDIUM
CVE-2026-47638	4.6 MEDIUM
CVE-2026-47639	5.4 MEDIUM
CVE-2026-47640	4.6 MEDIUM
CVE-2026-47641	4.6 MEDIUM
CVE-2026-48560	5.4 MEDIUM
CVE-2026-48562	4.6 MEDIUM

CWE's

CWE	Beschrijving
CWE-20	Improper Input Validation
CWE-22	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')
CWE-74	Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')
CWE-79	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')

CWE-121	Stack-based Buffer Overflow
CWE-122	Heap-based Buffer Overflow
CWE-125	Out-of-bounds Read
CWE-126	Buffer Over-read
CWE-190	Integer Overflow or Wraparound
CWE-191	Integer Underflow (Wrap or Wraparound)
CWE-197	Numeric Truncation Error
CWE-284	Improper Access Control
CWE-285	Improper Authorization
CWE-362	Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')
CWE-415	Double Free
CWE-416	Use After Free
CWE-502	Deserialization of Untrusted Data
CWE-693	Protection Mechanism Failure
CWE-822	Untrusted Pointer Dereference
CWE-843	Access of Resource Using Incompatible Type ('Type Confusion')

Getroffen producten

Microsoft
Microsoft 365 Apps for Enterprise for 32-bit Systems
Microsoft 365 Apps for Enterprise for 64-bit Systems
Microsoft Excel 2016 (32-bit edition)

Microsoft Excel 2016 (64-bit edition)
Microsoft Excel for Android
Microsoft Office 2016 (32-bit edition)
Microsoft Office 2016 (64-bit edition)
Microsoft Office 2019 for 32-bit editions
Microsoft Office 2019 for 64-bit editions
Microsoft Office 365 for Mac
Microsoft Office LTSC 2021 for 32-bit editions
Microsoft Office LTSC 2021 for 64-bit editions
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 Office for Android
Microsoft PowerPoint for Android
Microsoft SharePoint Enterprise Server 2016

Microsoft SharePoint Server 2019
Microsoft SharePoint Server Subscription Edition
Microsoft Teams for Android
Microsoft Word 2016 (32-bit edition)
Microsoft Word 2016 (64-bit edition)
Microsoft Word for Android
Office Online Server

Disclaimer