Nationaal Cyber Security Centrum
Ministerie van Justitie en Veiligheid

NCSC-2026-0286

Kwetsbaarheden verholpen in Microsoft Office

NCSC Security Advisory

PRIORITEIT: HOOG

Gepubliceerd op: 27-08-2026
Revisie: 1.0.1

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

Update Revisie 1

Er wordt actief misbruik gemeld van de kwetsbaarheid met kenmerk CVE-2026-63520 in Sharepoint.

Feiten

Microsoft heeft kwetsbaarheden verholpen in diverse Office producten.

Duiding

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

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

In onderstaande tabel wordt de kwetsbaarheid met kenmerk **CVE-2026-65667** genoemd met een CVSS score van 10.0. Ook worden de kwetsbaarheden met kenmerk **CVE-2026-50515, CVE-2026-62896** en **CVE-2026-70332** genoemd, elk met een CVSS score van 9 en hoger. Deze kwetsbaarheden zijn echter reeds centraal verholpen door microsoft en slechts opgenomen ter informatie. Hiervoor zijn geen acties vereist.

De kwetsbaarheid met kenmerk **CVE-2026-70306** heeft ook een CVSS score hoger dan 9 en vereist **wel** actie. Deze kwetsbaarheid bevindt zich in Sharepoint en stelt een kwaadwillende in staat om middels een Cross-site-scripting-aanval willekeurige code uit te voeren in de context van het slachtoffer.

UPDATE: Onderzoekers melden actief misbruik te hebben waargenomen van de kwetsbaarheid met kenmerk CVE-2026-63520. Deze bevindt zich in SharePoint en stelt een kwaadwillende in staat om willekeurige code uit te voeren op het kwetsbare systeem. Met name Sharepoint installaties die publiek toegankelijk zijn lopen hierdoor hoog risico op actief misbruik.

```
Microsoft OneDrive:
|----------------|------|-------------------------------------|
| CVE-ID         | CVSS | Impact                              |
|----------------|------|-------------------------------------|
| CVE-2026-65680 | 6.70 | Verkrijgen van verhoogde rechten    |
|----------------|------|-------------------------------------|

Azure SQL Managed Instance:
|----------------|------|-------------------------------------|
| CVE-ID         | CVSS | Impact                              |
|----------------|------|-------------------------------------|
| CVE-2026-62836 | 8.70 | Verkrijgen van verhoogde rechten    |
```

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

Microsoft Teams for Android:

CVE-ID	CVSS	Impact
CVE-2026-65768	8.80	Uitvoeren van willekeurige code
CVE-2026-65767	8.80	Voordoen als andere gebruiker

Microsoft Teams:

CVE-ID	CVSS	Impact
CVE-2026-62896	9.60	Verkrijgen van verhoogde rechten
CVE-2026-62918	7.50	Voordoen als andere gebruiker
CVE-2026-65667	10.0	Verkrijgen van verhoogde rechten

Microsoft Office Word:

CVE-ID	CVSS	Impact
CVE-2026-63518	7.80	Uitvoeren van willekeurige code
CVE-2026-63521	5.50	Toegang tot gevoelige gegevens
CVE-2026-70311	7.80	Uitvoeren van willekeurige code
CVE-2026-70310	5.50	Toegang tot gevoelige gegevens
CVE-2026-70319	5.50	Toegang tot gevoelige gegevens
CVE-2026-58651	7.80	Uitvoeren van willekeurige code
CVE-2026-63525	7.80	Uitvoeren van willekeurige code
CVE-2026-63528	5.50	Toegang tot gevoelige gegevens
CVE-2026-63527	7.80	Uitvoeren van willekeurige code
CVE-2026-63530	5.50	Toegang tot gevoelige gegevens
CVE-2026-63531	5.50	Toegang tot gevoelige gegevens
CVE-2026-64905	7.80	Uitvoeren van willekeurige code
CVE-2026-64907	7.80	Uitvoeren van willekeurige code
CVE-2026-64915	7.80	Uitvoeren van willekeurige code
CVE-2026-64917	5.50	Toegang tot gevoelige gegevens
CVE-2026-66806	5.50	Toegang tot gevoelige gegevens
CVE-2026-66810	5.50	Toegang tot gevoelige gegevens

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

Microsoft Office:

CVE-ID	CVSS	Impact
CVE-2026-63513	7.80	Uitvoeren van willekeurige code
CVE-2026-63515	7.80	Uitvoeren van willekeurige code
CVE-2026-63517	5.50	Toegang tot gevoelige gegevens
CVE-2026-63519	7.80	Uitvoeren van willekeurige code
CVE-2026-65657	7.80	Uitvoeren van willekeurige code
CVE-2026-65656	7.80	Uitvoeren van willekeurige code
CVE-2026-65661	7.80	Uitvoeren van willekeurige code
CVE-2026-65664	7.80	Uitvoeren van willekeurige code
CVE-2026-68792	7.80	Verkrijgen van verhoogde rechten
CVE-2026-70315	5.50	Toegang tot gevoelige gegevens
CVE-2026-70314	5.50	Toegang tot gevoelige gegevens
CVE-2026-70317	5.50	Toegang tot gevoelige gegevens
CVE-2026-70323	5.50	Toegang tot gevoelige gegevens
CVE-2026-62842	5.50	Toegang tot gevoelige gegevens
CVE-2026-63524	5.50	Toegang tot gevoelige gegevens
CVE-2026-63526	7.80	Uitvoeren van willekeurige code
CVE-2026-63529	5.50	Toegang tot gevoelige gegevens
CVE-2026-63532	7.80	Uitvoeren van willekeurige code
CVE-2026-63533	7.80	Uitvoeren van willekeurige code
CVE-2026-64898	7.80	Uitvoeren van willekeurige code
CVE-2026-64899	5.50	Toegang tot gevoelige gegevens
CVE-2026-64903	7.80	Uitvoeren van willekeurige code
CVE-2026-64904	7.80	Uitvoeren van willekeurige code
CVE-2026-64909	7.80	Uitvoeren van willekeurige code
CVE-2026-64910	7.80	Uitvoeren van willekeurige code
CVE-2026-64911	7.80	Uitvoeren van willekeurige code
CVE-2026-66807	7.80	Uitvoeren van willekeurige code
CVE-2026-66809	5.50	Toegang tot gevoelige gegevens
CVE-2026-70130	8.40	Uitvoeren van willekeurige code

Microsoft Office PowerPoint:

CVE-ID	CVSS	Impact
CVE-2026-68809	5.50	Toegang tot gevoelige gegevens

CVE-2026-70312	5.50	Toegang tot gevoelige gegevens
CVE-2026-70313	7.80	Toegang tot gevoelige gegevens
CVE-2026-70316	5.50	Toegang tot gevoelige gegevens
CVE-2026-70325	5.50	Toegang tot gevoelige gegevens
CVE-2026-70320	5.50	Toegang tot gevoelige gegevens
CVE-2026-70322	5.50	Toegang tot gevoelige gegevens

Microsoft Office Excel:

CVE-ID	CVSS	Impact
CVE-2026-65807	8.80	Uitvoeren van willekeurige code
CVE-2026-68793	7.80	Uitvoeren van willekeurige code
CVE-2026-68794	7.80	Uitvoeren van willekeurige code
CVE-2026-68795	7.80	Uitvoeren van willekeurige code
CVE-2026-68796	7.80	Uitvoeren van willekeurige code
CVE-2026-68800	7.80	Uitvoeren van willekeurige code
CVE-2026-68802	5.50	Toegang tot gevoelige gegevens
CVE-2026-68807	7.80	Uitvoeren van willekeurige code
CVE-2026-68806	7.80	Uitvoeren van willekeurige code
CVE-2026-68808	5.50	Toegang tot gevoelige gegevens
CVE-2026-68810	7.80	Uitvoeren van willekeurige code
CVE-2026-68811	7.80	Uitvoeren van willekeurige code
CVE-2026-68813	5.50	Toegang tot gevoelige gegevens
CVE-2026-68815	7.80	Uitvoeren van willekeurige code
CVE-2026-68816	7.80	Uitvoeren van willekeurige code
CVE-2026-70318	5.50	Toegang tot gevoelige gegevens
CVE-2026-70327	6.50	Toegang tot gevoelige gegevens
CVE-2026-70328	6.50	Toegang tot gevoelige gegevens
CVE-2026-68797	5.50	Toegang tot gevoelige gegevens
CVE-2026-68798	7.80	Uitvoeren van willekeurige code
CVE-2026-68799	5.50	Toegang tot gevoelige gegevens
CVE-2026-68801	7.80	Uitvoeren van willekeurige code
CVE-2026-68803	7.80	Uitvoeren van willekeurige code
CVE-2026-68804	7.80	Uitvoeren van willekeurige code
CVE-2026-68805	7.80	Uitvoeren van willekeurige code
CVE-2026-68812	7.80	Uitvoeren van willekeurige code
CVE-2026-68814	7.80	Uitvoeren van willekeurige code
CVE-2026-68817	7.80	Uitvoeren van willekeurige code

Microsoft Office Outlook:

CVE-ID	CVSS	Impact
CVE-2026-70329	8.80	Uitvoeren van willekeurige code
CVE-2026-62882	4.30	Voordoen als andere gebruiker

Azure Service Bus:

CVE-ID	CVSS	Impact
CVE-2026-50515	9.90	Uitvoeren van willekeurige code

Microsoft Office Access:

CVE-ID	CVSS	Impact
CVE-2026-64906	7.80	Uitvoeren van willekeurige code
CVE-2026-64912	7.80	Uitvoeren van willekeurige code
CVE-2026-64908	7.80	Uitvoeren van willekeurige code
CVE-2026-64914	7.80	Uitvoeren van willekeurige code
CVE-2026-64920	7.80	Uitvoeren van willekeurige code
CVE-2026-64919	7.80	Uitvoeren van willekeurige code

Microsoft Teams Mobile:

CVE-ID	CVSS	Impact
CVE-2026-65769	6.50	Toegang tot gevoelige gegevens

Microsoft Office SharePoint:

CVE-ID	CVSS	Impact
CVE-2026-57105	8.00	Voordoen als andere gebruiker
CVE-2026-62829	4.60	Voordoen als andere gebruiker

CVE-2026-62827	8.80	Verkrijgen van verhoogde rechten
CVE-2026-62837	6.50	Toegang tot gevoelige gegevens
CVE-2026-63514	8.80	Uitvoeren van willekeurige code
CVE-2026-63512	6.50	Manipulatie van gegevens
CVE-2026-63516	6.50	Voordoen als andere gebruiker
CVE-2026-63520	8.10	Uitvoeren van willekeurige code
CVE-2026-64922	4.60	Voordoen als andere gebruiker
CVE-2026-65658	8.80	Uitvoeren van willekeurige code
CVE-2026-65663	8.80	Uitvoeren van willekeurige code
CVE-2026-65660	6.50	Voordoen als andere gebruiker
CVE-2026-65665	8.80	Uitvoeren van willekeurige code
CVE-2026-70321	8.80	Uitvoeren van willekeurige code
CVE-2026-70324	8.80	Verkrijgen van verhoogde rechten
CVE-2026-70355	7.30	Verkrijgen van verhoogde rechten
CVE-2026-64897	4.60	Voordoen als andere gebruiker
CVE-2026-64900	4.60	Voordoen als andere gebruiker
CVE-2026-64902	4.60	Voordoen als andere gebruiker
CVE-2026-64901	8.80	Uitvoeren van willekeurige code
CVE-2026-64916	4.60	Voordoen als andere gebruiker
CVE-2026-64921	8.80	Verkrijgen van verhoogde rechten
CVE-2026-66805	8.80	Uitvoeren van willekeurige code
CVE-2026-66808	8.80	Uitvoeren van willekeurige code
CVE-2026-70306	9.30	Voordoen als andere gebruiker
CVE-2026-70326	8.80	Verkrijgen van verhoogde rechten
CVE-2026-70332	9.60	Voordoen als andere gebruiker
CVE-2026-58639	6.50	Voordoen als andere gebruiker
CVE-2026-62839	6.50	Voordoen als andere gebruiker
CVE-2026-62917	4.60	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-2026-65768	8.8 HIGH
CVE-2026-65767	8.8 HIGH
CVE-2026-57105	8.0 HIGH
CVE-2026-62829	4.6 MEDIUM
CVE-2026-62827	8.8 HIGH
CVE-2026-62837	6.5 MEDIUM
CVE-2026-63514	8.8 HIGH
CVE-2026-63512	6.5 MEDIUM
CVE-2026-63516	6.5 MEDIUM
CVE-2026-63520	8.1 HIGH
CVE-2026-64922	4.6 MEDIUM
CVE-2026-65658	8.8 HIGH
CVE-2026-65663	8.8 HIGH
CVE-2026-65660	6.5 MEDIUM
CVE-2026-65665	8.8 HIGH
CVE-2026-70324	8.8 HIGH
CVE-2026-70355	7.3 HIGH
CVE-2026-64897	4.6 MEDIUM
CVE-2026-64900	7.3 HIGH
CVE-2026-64902	4.6 MEDIUM
CVE-2026-64901	8.8 HIGH

CVE-2026-64916	4.6 MEDIUM
CVE-2026-64921	8.8 HIGH
CVE-2026-66805	8.8 HIGH
CVE-2026-66808	8.8 HIGH
CVE-2026-70306	9.3 CRITICAL
CVE-2026-58639	6.5 MEDIUM
CVE-2026-62839	6.5 MEDIUM
CVE-2026-62917	4.6 MEDIUM
CVE-2026-70321	8.8 HIGH
CVE-2026-70326	8.8 HIGH
CVE-2026-62896	9.6 CRITICAL
CVE-2026-62918	7.5 HIGH
CVE-2026-65667	10.0 CRITICAL
CVE-2026-62836	8.7 HIGH
CVE-2026-50515	9.9 CRITICAL
CVE-2026-63513	7.8 HIGH
CVE-2026-63515	7.8 HIGH
CVE-2026-63518	7.8 HIGH
CVE-2026-63521	5.5 MEDIUM
CVE-2026-63519	7.8 HIGH
CVE-2026-65657	7.8 HIGH
CVE-2026-65656	7.8 HIGH
CVE-2026-65661	7.8 HIGH

CVE-2026-65664	7.8 HIGH
CVE-2026-65807	8.8 HIGH
CVE-2026-68792	7.8 HIGH
CVE-2026-68793	7.8 HIGH
CVE-2026-68794	7.8 HIGH
CVE-2026-68795	7.8 HIGH
CVE-2026-68796	7.8 HIGH
CVE-2026-68800	7.8 HIGH
CVE-2026-68802	5.5 MEDIUM
CVE-2026-68807	7.8 HIGH
CVE-2026-68806	7.8 HIGH
CVE-2026-68808	5.5 MEDIUM
CVE-2026-68809	5.5 MEDIUM
CVE-2026-68810	7.8 HIGH
CVE-2026-68811	7.8 HIGH
CVE-2026-68813	5.5 MEDIUM
CVE-2026-68815	7.8 HIGH
CVE-2026-68816	7.8 HIGH
CVE-2026-70312	5.5 MEDIUM
CVE-2026-70311	7.8 HIGH
CVE-2026-70313	7.8 HIGH
CVE-2026-70310	5.5 MEDIUM
CVE-2026-70316	5.5 MEDIUM

CVE-2026-70315	5.5 MEDIUM
CVE-2026-70318	5.5 MEDIUM
CVE-2026-70314	5.5 MEDIUM
CVE-2026-70317	5.5 MEDIUM
CVE-2026-70325	5.5 MEDIUM
CVE-2026-70319	5.5 MEDIUM
CVE-2026-70320	5.5 MEDIUM
CVE-2026-70323	5.5 MEDIUM
CVE-2026-70322	5.5 MEDIUM
CVE-2026-70327	6.5 MEDIUM
CVE-2026-70328	6.5 MEDIUM
CVE-2026-70329	8.8 HIGH
CVE-2026-62842	5.5 MEDIUM
CVE-2026-63524	5.5 MEDIUM
CVE-2026-63525	7.8 HIGH
CVE-2026-63526	7.8 HIGH
CVE-2026-63528	5.5 MEDIUM
CVE-2026-63527	7.8 HIGH
CVE-2026-63529	5.5 MEDIUM
CVE-2026-63530	5.5 MEDIUM
CVE-2026-63531	5.5 MEDIUM
CVE-2026-63532	7.8 HIGH
CVE-2026-63533	7.8 HIGH

CVE-2026-64898	7.8 HIGH
CVE-2026-64899	5.5 MEDIUM
CVE-2026-64903	7.8 HIGH
CVE-2026-64904	7.8 HIGH
CVE-2026-64905	7.8 HIGH
CVE-2026-64907	7.8 HIGH
CVE-2026-64906	7.8 HIGH
CVE-2026-64909	7.8 HIGH
CVE-2026-64910	7.8 HIGH
CVE-2026-64912	7.8 HIGH
CVE-2026-64911	7.8 HIGH
CVE-2026-64908	7.8 HIGH
CVE-2026-64914	7.8 HIGH
CVE-2026-64915	7.8 HIGH
CVE-2026-64920	7.8 HIGH
CVE-2026-64917	5.5 MEDIUM
CVE-2026-64919	7.8 HIGH
CVE-2026-62882	4.3 MEDIUM
CVE-2026-66806	7.4 HIGH
CVE-2026-66807	7.8 HIGH
CVE-2026-66810	5.5 MEDIUM
CVE-2026-66809	5.5 MEDIUM
CVE-2026-68797	5.5 MEDIUM

CVE-2026-68799	5.5 MEDIUM
CVE-2026-68801	7.8 HIGH
CVE-2026-68803	7.8 HIGH
CVE-2026-68804	7.8 HIGH
CVE-2026-68805	7.8 HIGH
CVE-2026-68812	7.8 HIGH
CVE-2026-68814	7.8 HIGH
CVE-2026-68817	7.8 HIGH
CVE-2026-70130	8.4 HIGH
CVE-2026-63517	5.5 MEDIUM
CVE-2026-58651	7.8 HIGH
CVE-2026-68798	7.8 HIGH
CVE-2026-65769	6.5 MEDIUM
CVE-2026-65680	6.7 MEDIUM
CVE-2026-70332	9.6 CRITICAL

CWE's

CWE	Beschrijving
CWE-20	Improper Input Validation
CWE-22	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')
CWE-23	Relative Path Traversal
CWE-59	Improper Link Resolution Before File Access ('Link Following')
CWE-77	Improper Neutralization of Special Elements used in a Command ('Command Injection')

CWE-79	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')
CWE-88	Improper Neutralization of Argument Delimiters in a Command ('Argument Injection')
CWE-94	Improper Control of Generation of Code ('Code Injection')
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-193	Off-by-one Error
CWE-197	Numeric Truncation Error
CWE-200	Exposure of Sensitive Information to an Unauthorized Actor
CWE-287	Improper Authentication
CWE-295	Improper Certificate Validation
CWE-306	Missing Authentication for Critical Function
CWE-347	Improper Verification of Cryptographic Signature
CWE-416	Use After Free
CWE-459	Incomplete Cleanup
CWE-502	Deserialization of Untrusted Data
CWE-522	Insufficiently Protected Credentials
CWE-787	Out-of-bounds Write
CWE-822	Untrusted Pointer Dereference
CWE-843	Access of Resource Using Incompatible Type ('Type Confusion')
CWE-862	Missing Authorization
CWE-863	Incorrect Authorization

CWE-908	Use of Uninitialized Resource
CWE-918	Server-Side Request Forgery (SSRF)
CWE-923	Improper Restriction of Communication Channel to Intended Endpoints

Getroffen producten

Microsoft
Microsoft 365 Apps for Enterprise for 32-bit Systems
Microsoft 365 Apps for Enterprise for 64-bit Systems
Microsoft Access 2016 (32-bit edition)
Microsoft Access 2016 (64-bit edition)
Microsoft Excel 2016 (32-bit edition)
Microsoft Excel 2016 (64-bit edition)
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 Outlook 2016 (32-bit edition)
Microsoft Outlook 2016 (64-bit edition)
Microsoft PowerPoint 2016 (32-bit edition)
Microsoft PowerPoint 2016 (64-bit edition)
Microsoft SharePoint Enterprise Server 2016
Microsoft SharePoint Online
Microsoft SharePoint Server 2019
Microsoft SharePoint Server Subscription Edition
Microsoft Teams
Microsoft Teams for Android
Microsoft Teams for iOS

Microsoft Word 2016 (32-bit edition)
Microsoft Word 2016 (64-bit edition)
OneDrive for MacOS
Service Bus
SharePoint
teams

Disclaimer