Nationaal Cyber Security Centrum
Ministerie van Justitie en Veiligheid

NCSC-2025-0278

Kwetsbaarheden verholpen in Microsoft Office

NCSC Advisory
Prioriteit: Normaal
Gepubliceerd op: 09-09-2025

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 aanvallen uit te voeren die kunnen leiden tot de volgende categorieën schade:

- Uitvoeren van willekeurige code (Gebruikersrechten)
- Toegang tot gevoelige gegevens
- Verkrijgen van verhoogde rechten
- Voordoen als andere gebruiker

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

Microsoft Office:

CVE-ID	CVSS	Impact
CVE-2025-54906	7.80	Uitvoeren van willekeurige code
CVE-2025-55243	7.50	Voordoen als andere gebruiker
CVE-2025-54910	8.40	Uitvoeren van willekeurige code

Microsoft Office Word:

CVE-ID	CVSS	Impact
CVE-2025-54905	7.10	Toegang tot gevoelige gegevens

Microsoft Office Visio:

CVE-ID	CVSS	Impact
CVE-2025-54907	7.80	Uitvoeren van willekeurige code

Windows Imaging Component:

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

CVE-ID	CVSS	Impact
CVE-2025-53799	5.50	Toegang tot gevoelige gegevens

Microsoft Office PowerPoint:

CVE-ID	CVSS	Impact
CVE-2025-54908	7.80	Uitvoeren van willekeurige code

Microsoft AutoUpdate (MAU):

CVE-ID	CVSS	Impact
CVE-2025-55317	7.80	Verkrijgen van verhoogde rechten

Microsoft Office SharePoint:

CVE-ID	CVSS	Impact
CVE-2025-54897	8.80	Uitvoeren van willekeurige code

Microsoft Office Excel:

CVE-ID	CVSS	Impact
CVE-2025-54896	7.80	Uitvoeren van willekeurige code
CVE-2025-54898	7.80	Uitvoeren van willekeurige code
CVE-2025-54899	7.80	Uitvoeren van willekeurige code
CVE-2025-54902	7.80	Uitvoeren van willekeurige code
CVE-2025-54903	7.80	Uitvoeren van willekeurige code
CVE-2025-54904	7.80	Uitvoeren van willekeurige code
CVE-2025-54900	7.80	Uitvoeren van willekeurige code
CVE-2025-54901	5.50	Toegang tot gevoelige gegevens

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-2025-54896	7.8 HIGH
CVE-2025-54898	7.8 HIGH
CVE-2025-54902	7.8 HIGH
CVE-2025-54903	7.8 HIGH
CVE-2025-54904	7.8 HIGH
CVE-2025-54900	7.8 HIGH
CVE-2025-54899	7.8 HIGH
CVE-2025-54905	7.1 HIGH
CVE-2025-54906	7.8 HIGH
CVE-2025-54907	7.8 HIGH
CVE-2025-54908	7.8 HIGH
CVE-2025-54901	5.5 MEDIUM
CVE-2025-54910	8.4 HIGH
CVE-2025-54897	8.8 HIGH
CVE-2025-55243	
CVE-2025-55317	7.8 HIGH

CVE-2025-53799	**5.5 MEDIUM**

CWE's

CWE	Beschrijving
CWE-59	Improper Link Resolution Before File Access ('Link Following')
CWE-122	Heap-based Buffer Overflow
CWE-125	Out-of-bounds Read
CWE-126	Buffer Over-read
CWE-200	Exposure of Sensitive Information to an Unauthorized Actor
CWE-416	Use After Free
CWE-502	Deserialization of Untrusted Data
CWE-590	Free of Memory not on the Heap
CWE-822	Untrusted Pointer Dereference
CWE-908	Use of Uninitialized Resource

Getroffen producten

Microsoft
Microsoft 365 Apps for Enterprise
Microsoft AutoUpdate for Mac
Microsoft Excel 2016
Microsoft Office 2016
Microsoft Office 2019

Microsoft Office LTSC 2021
Microsoft Office LTSC 2024
Microsoft Office LTSC for Mac 2021
Microsoft Office LTSC for Mac 2024
Microsoft Office for Android
Microsoft OfficePLUS
Microsoft PowerPoint 2016
Microsoft SharePoint Enterprise Server 2016
Microsoft SharePoint Server 2019
Microsoft SharePoint Server Subscription Edition
Microsoft Word 2016
Office Online Server

Disclaimer