Nationaal Cyber Security Centrum
Ministerie van Justitie en Veiligheid

NCSC-2025-0155

Kwetsbaarheden verholpen in Microsoft Office

NCSC Advisory
Prioriteit: Normaal
Gepubliceerd op: 13-05-2025

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 zich verhoogde rechten toe te kennen en willekeurige code uit te voeren met rechten van het slachtoffer.

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

Microsoft Office PowerPoint:

CVE-ID	CVSS	Impact
CVE-2025-29978	7.80	Uitvoeren van willekeurige code

Microsoft Office Outlook:

CVE-ID	CVSS	Impact
CVE-2025-32705	7.80	Uitvoeren van willekeurige code

Microsoft Office:

CVE-ID	CVSS	Impact
CVE-2025-30377	8.40	Uitvoeren van willekeurige code
CVE-2025-30386	8.40	Uitvoeren van willekeurige code

Microsoft Office SharePoint:

CVE-ID	CVSS	Impact
CVE-2025-29976	7.80	Verkrijgen van verhoogde rechten
CVE-2025-30378	7.00	Uitvoeren van willekeurige code
CVE-2025-30382	7.80	Uitvoeren van willekeurige code

```
| CVE-2025-30384 | 7.40 | Uitvoeren van willekeurige code     |
|----------------|------|-------------------------------------|

Microsoft Office Excel:
|----------------|------|-------------------------------------|
| CVE-ID         | CVSS | Impact                              |
|----------------|------|-------------------------------------|
| CVE-2025-29977 | 7.80 | Uitvoeren van willekeurige code     |
| CVE-2025-29979 | 7.80 | Uitvoeren van willekeurige code     |
| CVE-2025-30375 | 7.80 | Uitvoeren van willekeurige code     |
| CVE-2025-30376 | 7.80 | Uitvoeren van willekeurige code     |
| CVE-2025-30379 | 7.80 | Uitvoeren van willekeurige code     |
| CVE-2025-30381 | 7.80 | Uitvoeren van willekeurige code     |
| CVE-2025-30383 | 7.80 | Uitvoeren van willekeurige code     |
| CVE-2025-30393 | 7.80 | Uitvoeren van willekeurige code     |
| CVE-2025-32704 | 8.40 | Uitvoeren van willekeurige code     |
|----------------|------|-------------------------------------|

Windows Win32K - GRFX:
|----------------|------|-------------------------------------|
| CVE-ID         | CVSS | Impact                              |
|----------------|------|-------------------------------------|
| CVE-2025-30388 | 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-2025-29976	
CVE-2025-30378	7.0 HIGH

CVE-2025-30382	
CVE-2025-30384	
CVE-2025-29977	
CVE-2025-29979	7.8 HIGH
CVE-2025-30375	
CVE-2025-30376	7.8 HIGH
CVE-2025-30379	
CVE-2025-30381	
CVE-2025-30383	7.8 HIGH
CVE-2025-30377	
CVE-2025-30386	8.4 HIGH
CVE-2025-32704	
CVE-2025-29978	
CVE-2025-30393	7.8 HIGH
CVE-2025-32705	
CVE-2025-30388	7.8 HIGH

CWE's

CWE	Beschrijving
CWE-763	Release of Invalid Pointer or Reference
CWE-822	Untrusted Pointer Dereference
CWE-126	Buffer Over-read
CWE-843	Access of Resource Using Incompatible Type ('Type Confusion')
CWE-125	Out-of-bounds Read

CWE-416	Use After Free
CWE-502	Deserialization of Untrusted Data
CWE-122	Heap-based Buffer Overflow
CWE-269	Improper Privilege Management

Getroffen producten

Microsoft
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 LTSC for Mac 2021
Microsoft Office LTSC for Mac 2024
Microsoft Office LTSC 2021 for 32-bit editions
Microsoft Office LTSC 2024 for 32-bit editions
Microsoft Office LTSC 2024 for 64-bit editions

Microsoft SharePoint Server Subscription Edition
Microsoft SharePoint Server 2019
Microsoft SharePoint Enterprise Server 2016
Microsoft 365 Apps for Enterprise for 32-bit Systems
Microsoft 365 Apps for Enterprise for 64-bit Systems
Office
powerpoint
sharepoint_server

Disclaimer