Nationaal Cyber Security Centrum
Ministerie van Justitie en Veiligheid

NCSC-2025-0250

Kwetsbaarheden verholpen in Microsoft Office

NCSC Advisory
Prioriteit: Normaal
Gepubliceerd op: 13-08-2025

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 Microsoft Office (inclusief SharePoint, Visio, Word, Excel en PowerPoint).

Duiding

De kwetsbaarheden in Microsoft Office omvatten verschillende 'use after free'-fouten, heap-gebaseerde bufferoverflows en andere kwetsbaarheden die ongeautoriseerde aanvallers in staat stellen om willekeurige code uit te voeren op lokale machines. Deze kwetsbaarheden kunnen worden geëxploiteerd via speciaal vervaardigde documenten of door misbruik van onbetrouwbare gegevens, wat kan leiden tot ongeautoriseerde toegang en controle over systemen.

Microsoft Teams:

CVE-ID	CVSS	Impact
CVE-2025-53783	7.50	Uitvoeren van willekeurige code

Microsoft Office PowerPoint:

CVE-ID	CVSS	Impact
CVE-2025-53761	7.80	Uitvoeren van willekeurige code

Windows GDI+:

CVE-ID	CVSS	Impact
CVE-2025-53766	9.80	Uitvoeren van willekeurige code

Microsoft Office Word:

CVE-ID	CVSS	Impact
CVE-2025-53733	8.40	Uitvoeren van willekeurige code
CVE-2025-53736	6.80	Toegang tot gevoelige gegevens
CVE-2025-53738	7.80	Uitvoeren van willekeurige code
CVE-2025-53784	8.40	Uitvoeren van willekeurige code

Microsoft Office Visio:

CVE-ID	CVSS	Impact
CVE-2025-53730	7.80	Uitvoeren van willekeurige code
CVE-2025-53734	7.80	Uitvoeren van willekeurige code

Microsoft Office:

CVE-ID	CVSS	Impact
CVE-2025-53731	8.40	Uitvoeren van willekeurige code
CVE-2025-53732	7.80	Uitvoeren van willekeurige code
CVE-2025-53740	8.40	Uitvoeren van willekeurige code

Microsoft Office SharePoint:

CVE-ID	CVSS	Impact
CVE-2025-53760	7.10	Verkrijgen van verhoogde rechten
CVE-2025-49712	8.80	Uitvoeren van willekeurige code

Microsoft Office Excel:

CVE-ID	CVSS	Impact
CVE-2025-53741	7.80	Uitvoeren van willekeurige code
CVE-2025-53759	7.80	Uitvoeren van willekeurige code
CVE-2025-53735	7.80	Uitvoeren van willekeurige code
CVE-2025-53737	7.80	Uitvoeren van willekeurige code
CVE-2025-53739	7.80	Uitvoeren van willekeurige code

Oplossingen

Microsoft heeft updates uitgebracht om de kwetsbaarheden te verhelpen. Zie bijgevoegde referenties voor meer informatie.

Referenties

- https://msrc.microsoft.com/update-guide/en-us

Kwetsbaarheden

CVE	CVSS Score
CVE-2025-49712	
CVE-2025-53730	7.8 HIGH
CVE-2025-53731	8.4 HIGH
CVE-2025-53732	
CVE-2025-53733	
CVE-2025-53734	
CVE-2025-53735	7.8 HIGH
CVE-2025-53736	
CVE-2025-53737	7.8 HIGH
CVE-2025-53738	7.8 HIGH
CVE-2025-53739	
CVE-2025-53740	8.4 HIGH
CVE-2025-53741	7.8 HIGH
CVE-2025-53759	7.8 HIGH
CVE-2025-53760	7.1 HIGH
CVE-2025-53761	7.8 HIGH
CVE-2025-53766	9.8 CRITICAL
CVE-2025-53783	7.5 HIGH
CVE-2025-53784	8.4 HIGH

CWE's

CWE	Beschrijving
CWE-126	Buffer Over-read
CWE-908	Use of Uninitialized Resource
CWE-843	Access of Resource Using Incompatible Type ('Type Confusion')
CWE-416	Use After Free
CWE-502	Deserialization of Untrusted Data
CWE-918	Server-Side Request Forgery (SSRF)
CWE-122	Heap-based Buffer Overflow
CWE-681	Incorrect Conversion between Numeric Types

Getroffen producten

Microsoft
365 Apps
Excel
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 (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 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 Excel 2016
Microsoft Office 2016
Microsoft Office 2019
Microsoft Office LTSC 2021
Microsoft Office LTSC 2024

Disclaimer