Nationaal Cyber Security Centrum
Ministerie van Justitie en Veiligheid

NCSC-2025-0107

Kwetsbaarheden verholpen in Microsoft Office

NCSC Advisory
Prioriteit: Normaal
Gepubliceerd op: 08-04-2025

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 willekeurige code uit te voeren in de context van het slachtoffer en daarmee mogelijk toegang krijgen tot gevoelige gegevens.

De kwetsbaarheid met kenmerk CVE-2025-29794 in Microsoft SharePoint stelt een kwaadwillende in staat om willekeurige code over een netwerk uit te voeren. Een geauthenticeerde kwaadwillende kan deze kwetsbaarheid misbruiken, en hiervoor zijn geen verhoogde rechten vereist.

De kwetsbaarheid met kenmerk CVE-2025-29822 in Microsoft OneNote stelt een kwaadwillende in staat om lokaal een beveiligingsfunctie te omzeilen. Voor succesvol misbruik moet de kwaadwillende het slachtoffer misleiden om een malafide bestand te openen en vervolgens op een speciaal vervaardigde URL te klikken.

Microsoft Office:

CVE-ID	CVSS	Impact
CVE-2025-27744	7,80	Verkrijgen van verhoogde rechten
CVE-2025-27745	7,80	Uitvoeren van willekeurige code
CVE-2025-27746	7,80	Uitvoeren van willekeurige code
CVE-2025-27748	7,80	Uitvoeren van willekeurige code
CVE-2025-27749	7,80	Uitvoeren van willekeurige code
CVE-2025-29792	7,30	Verkrijgen van verhoogde rechten
CVE-2025-26642	7,80	Uitvoeren van willekeurige code
CVE-2025-29791	7,80	Uitvoeren van willekeurige code

Microsoft Office Word:

CVE-ID	CVSS	Impact
CVE-2025-27747	7,80	Uitvoeren van willekeurige code
CVE-2025-29816	7,50	Omzeilen van beveiligingsmaatregel
CVE-2025-29820	7,80	Uitvoeren van willekeurige code

Microsoft Office OneNote:

CVE-ID	CVSS	Impact
CVE-2025-29822	7,80	Omzeilen van beveiligingsmaatregel

Microsoft AutoUpdate (MAU):

CVE-ID	CVSS	Impact
CVE-2025-29800	7,80	Verkrijgen van verhoogde rechten
CVE-2025-29801	7,80	Verkrijgen van verhoogde rechten

Microsoft Office SharePoint:

CVE-ID	CVSS	Impact
CVE-2025-29793	7,20	Uitvoeren van willekeurige code
CVE-2025-29794	8,80	Uitvoeren van willekeurige code

Microsoft Office Excel:

CVE-ID	CVSS	Impact
CVE-2025-27750	7,80	Uitvoeren van willekeurige code
CVE-2025-27752	7,80	Uitvoeren van willekeurige code
CVE-2025-27751	7,80	Uitvoeren van willekeurige code
CVE-2025-29823	7,80	Uitvoeren van willekeurige code

Windows Win32K - GRFX:

CVE-ID	CVSS	Impact
CVE-2025-26687	7,50	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

Dreigingsinformatie

Kwetsbaarheden

CVE	CVSS Score
CVE-2025-26642	7.8 HIGH
CVE-2025-26687	7.5 HIGH
CVE-2025-27744	7.8 HIGH
CVE-2025-27745	7.8 HIGH
CVE-2025-27746	7.8 HIGH
CVE-2025-27747	7.8 HIGH
CVE-2025-27748	7.8 HIGH
CVE-2025-27749	7.8 HIGH
CVE-2025-27750	7.8 HIGH
CVE-2025-27751	7.8 HIGH
CVE-2025-27752	7.8 HIGH
CVE-2025-29791	7.8 HIGH
CVE-2025-29792	7.3 HIGH
CVE-2025-29793	7.2 HIGH
CVE-2025-29794	8.8 HIGH

CVE-2025-29800	7.8 HIGH
CVE-2025-29801	7.8 HIGH
CVE-2025-29816	7.5 HIGH
CVE-2025-29820	7.8 HIGH
CVE-2025-29822	7.8 HIGH
CVE-2025-29823	7.8 HIGH

CWE's

CWE	Beschrijving
CWE-184	Incomplete List of Disallowed Inputs
CWE-822	Untrusted Pointer Dereference
CWE-349	Acceptance of Extraneous Untrusted Data With Trusted Data
CWE-843	Access of Resource Using Incompatible Type ('Type Confusion')
CWE-190	Integer Overflow or Wraparound
CWE-285	Improper Authorization
CWE-125	Out-of-bounds Read
CWE-284	Improper Access Control
CWE-416	Use After Free
CWE-502	Deserialization of Untrusted Data
CWE-122	Heap-based Buffer Overflow
CWE-269	Improper Privilege Management
CWE-276	Incorrect Default Permissions

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 AutoUpdate for Mac
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 Office LTSC for Mac 2024
Microsoft Office for Android
Microsoft Office for Universal
Microsoft OneNote 2016 (32-bit edition)
Microsoft OneNote 2016 (64-bit edition)
Microsoft OneNote for Mac
Microsoft SharePoint Enterprise Server 2016
Microsoft SharePoint Server 2019
Microsoft SharePoint Server Subscription Edition
Microsoft Word 2016 (32-bit edition)
Microsoft Word 2016 (64-bit edition)
Office Online Server
SharePoint Server Subscription Edition Language Pack
Windows 10 Version 1607 for 32-bit Systems
Windows 10 Version 1607 for x64-based Systems

Windows 10 Version 1809 for 32-bit Systems
Windows 10 Version 1809 for x64-based Systems
Windows 10 Version 21H2 for 32-bit Systems
Windows 10 Version 21H2 for ARM64-based Systems
Windows 10 Version 21H2 for x64-based Systems
Windows 10 Version 22H2 for 32-bit Systems
Windows 10 Version 22H2 for ARM64-based Systems
Windows 10 Version 22H2 for x64-based Systems
Windows 10 for 32-bit Systems
Windows 10 for x64-based Systems
Windows 11 Version 22H2 for ARM64-based Systems
Windows 11 Version 22H2 for x64-based Systems
Windows 11 Version 23H2 for ARM64-based Systems
Windows 11 Version 23H2 for x64-based Systems
Windows 11 Version 24H2 for ARM64-based Systems
Windows 11 Version 24H2 for x64-based Systems

Windows Server 2016
Windows Server 2016 (Server Core installation)
Windows Server 2019
Windows Server 2019 (Server Core installation)
Windows Server 2022
Windows Server 2022 (Server Core installation)
Windows Server 2022, 23H2 Edition (Server Core installation)
Windows Server 2025
Windows Server 2025 (Server Core installation)
Windows Server 2008 R2 for x64-based Systems Service Pack 1
Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation)
Windows Server 2008 for 32-bit Systems Service Pack 2
Windows Server 2008 for 32-bit Systems Service Pack 2 (Server Core installation)
Windows Server 2008 for x64-based Systems Service Pack 2
Windows Server 2008 for x64-based Systems Service Pack 2 (Server Core installation)
Windows Server 2012

Windows Server 2012 (Server Core installation)
Windows Server 2012 R2
Windows Server 2012 R2 (Server Core installation)

Disclaimer