Nationaal Cyber Security Centrum
Ministerie van Justitie en Veiligheid

NCSC-2026-0352

Kwetsbaarheden verholpen in Microsoft Office

NCSC Security Advisory
Prioriteit: Normaal
Gepubliceerd op: 08-09-2026

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 114 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 genoemd in onderstaande tabel.

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

Microsoft heeft voor Office 114 kwetsbaarheden verholpen. De 4 ernstigste kwetsbaarheden bevinden zich in meerdere Office componenten en hebben een CVSS score van 9.8 toegewezen gekregen. Kwaadwillenden met toegang tot deze componenten kunnen zonder voorafgaande authenticatie mogelijk code uitvoeren of zich toegang verschaffen tot het kwetsbare systeem. Deze kwetsbaarheden zijn in onderstaande tabel weergegeven.

De overige 110 kwetsbaarheden variëren in ernst van middelmatig tot hoog en kritiek. Raapleeg het MSRC-portaal voor aanvullende informatie.

CVE-ID	CVSS	Component	Impact
CVE-2026-78505	9,80	Office	Uitvoeren van willekeurige code
CVE-2026-78509	9,80	Outlook	Uitvoeren van willekeurige code
CVE-2026-78510	9,80	Outlook	Uitvoeren van willekeurige code
CVE-2026-66302	9,80	SKYPE	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

Referenties

- https://portal.msrc.microsoft.com/en-us/security-guidance

Kwetsbaarheden

CVE	CVSS Score
CVE-2026-62804	
CVE-2026-63523	
CVE-2026-64918	
CVE-2026-66302	
CVE-2026-66303	
CVE-2026-66304	
CVE-2026-66305	
CVE-2026-66306	
CVE-2026-66307	
CVE-2026-66308	
CVE-2026-69268	
CVE-2026-69273	
CVE-2026-69282	
CVE-2026-69285	
CVE-2026-69402	
CVE-2026-69409	
CVE-2026-69417	
CVE-2026-69442	

- CVE-2026-69464
- CVE-2026-69465
- CVE-2026-69477
- CVE-2026-69529
- CVE-2026-69559
- CVE-2026-69614
- CVE-2026-69615
- CVE-2026-69626
- CVE-2026-69629
- CVE-2026-69632
- CVE-2026-69636
- CVE-2026-69642
- CVE-2026-69646
- CVE-2026-69671
- CVE-2026-69678
- CVE-2026-69683
- CVE-2026-69686
- CVE-2026-69690
- CVE-2026-69716
- CVE-2026-69719
- CVE-2026-69722
- CVE-2026-69724
- CVE-2026-69734

- CVE-2026-69739
- CVE-2026-69742
- CVE-2026-69759
- CVE-2026-69764
- CVE-2026-69767
- CVE-2026-69778
- CVE-2026-69797
- CVE-2026-69804
- CVE-2026-69904
- CVE-2026-72938
- CVE-2026-72956
- CVE-2026-72972
- CVE-2026-72973
- CVE-2026-72974
- CVE-2026-72975
- CVE-2026-72976
- CVE-2026-72977
- CVE-2026-77898
- CVE-2026-78439
- CVE-2026-78502
- CVE-2026-78503
- CVE-2026-78504
- CVE-2026-78505

- CVE-2026-78506
- CVE-2026-78507
- CVE-2026-78509
- CVE-2026-78510
- CVE-2026-78511
- CVE-2026-78512
- CVE-2026-78513
- CVE-2026-78514
- CVE-2026-78515
- CVE-2026-78517
- CVE-2026-78526
- CVE-2026-80076
- CVE-2026-80078
- CVE-2026-80082
- CVE-2026-80084
- CVE-2026-80086
- CVE-2026-80087
- CVE-2026-80089
- CVE-2026-80091
- CVE-2026-81385
- CVE-2026-81386
- CVE-2026-81387
- CVE-2026-81388

- CVE-2026-81389
- CVE-2026-81390
- CVE-2026-81391
- CVE-2026-81392
- CVE-2026-81393
- CVE-2026-81394
- CVE-2026-81395
- CVE-2026-81396
- CVE-2026-81397
- CVE-2026-81398
- CVE-2026-81399
- CVE-2026-81400
- CVE-2026-81401
- CVE-2026-81947
- CVE-2026-81948
- CVE-2026-81949
- CVE-2026-81950
- CVE-2026-81951
- CVE-2026-81952
- CVE-2026-81953
- CVE-2026-81954
- CVE-2026-81955
- CVE-2026-81956

- CVE-2026-81957
- CVE-2026-81958
- CVE-2026-81959
- CVE-2026-81960

CWE's

CWE	Beschrijving
CWE-73	External Control of File Name or Path
CWE-79	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')
CWE-89	Improper Neutralization of Special Elements used in an SQL Command ('SQL 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-170	Improper Null Termination
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-209	Generation of Error Message Containing Sensitive Information
CWE-250	Execution with Unnecessary Privileges
CWE-346	Origin Validation Error
CWE-347	Improper Verification of Cryptographic Signature
CWE-367	Time-of-check Time-of-use (TOCTOU) Race Condition

CWE-415	Double Free
CWE-416	Use After Free
CWE-476	NULL Pointer Dereference
CWE-497	Exposure of Sensitive System Information to an Unauthorized Control Sphere
CWE-502	Deserialization of Untrusted Data
CWE-522	Insufficiently Protected Credentials
CWE-603	Use of Client-Side Authentication
CWE-822	Untrusted Pointer Dereference
CWE-843	Access of Resource Using Incompatible Type ('Type Confusion')
CWE-862	Missing Authorization
CWE-908	Use of Uninitialized Resource
CWE-918	Server-Side Request Forgery (SSRF)

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 Office for Android
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 Publisher 2016 (32-bit edition)
Microsoft Publisher 2016 (64-bit edition)
Microsoft SharePoint Enterprise Server 2016

Disclaimer