Nationaal Cyber Security Centrum
Ministerie van Justitie en Veiligheid

NCSC-2026-0039

ZeroDay kwetsbaarheid verholpen in Microsoft Office

NCSC Advisory
Prioriteit: Normaal
Gepubliceerd op: 27-01-2026

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 een ZeroDay kwetsbaarheid verholpen in Microsoft Office.

Duiding

De kwetsbaarheid bevindt zich in de wijze waarop Microsoft Office omgaat met onbetrouwbare invoer, wat aanvallers in staat stelt om beveiligingsfuncties lokaal te omzeilen. Dit kan de integriteit van beveiligingsbeslissingen die door de software worden genomen, beïnvloeden. De afhankelijkheid van onbetrouwbare invoer creëert een pad voor potentiële exploitatie, wat kan leiden tot ongeautoriseerde toegang of acties binnen de getroffen systemen.

Voor succesvol misbruik moet de kwaadwillende lokale toegang tot het kwetsbare systeem hebben. Dit kan ook mogelijk worden verwezenlijkt door het slachtoffer te misleiden een malafide document te openen.

Microsoft geeft aan op de hoogte te zijn dat exploitcode gedeeld wordt. De exploitcode is (nog) niet publiek beschikbaar. Het Amerikaanse CISA heeft de kwetsbaarheid op de Known Exploited Vulnerabilities-lijst geplaatst, wat inhoudt dat misbruik van de kwetsbaarheid is bevestigd bij een Amerikaanse Federale overheids-organisatie.

Oplossingen

Microsoft heeft updates uitgebracht om de kwetsbaarheid te verhelpen voor Office 2021. Voor Office 2016 en 2019 zijn (nog) geen updates beschikbaar, maar deze worden zeer spoedig verwacht. Wel zijn er mitigerende maatregelen beschikbaar om het risico van misbruik zoveel mogelijk te beperken. Zie bijgevoegde referenties voor meer informatie.

Referenties

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-21509

Kwetsbaarheden

CVE	CVSS Score
CVE-2026-21509	7.8 HIGH

CWE's

CWE	Beschrijving
CWE-807	Reliance on Untrusted Inputs in a Security Decision

Getroffen producten

Microsoft
Microsoft 365 Apps for Enterprise
Microsoft 365 Apps for Enterprise for 32-bit Systems
Microsoft 365 Apps for Enterprise for 64-bit Systems
Microsoft Office 2016
Microsoft Office 2016 (32-bit edition)
Microsoft Office 2016 (64-bit edition)
Microsoft Office 2019
Microsoft Office 2019 for 32-bit editions
Microsoft Office 2019 for 64-bit editions
Microsoft Office LTSC 2021
Microsoft Office LTSC 2021 for 32-bit editions
Microsoft Office LTSC 2021 for 64-bit editions

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

Disclaimer