



NCSC-2025-0215

Kwetsbaarheden verholpen in Microsoft Office

NCSC Advisory

PRIORITEIT: HOOG

Gepubliceerd op: 19-07-2025

Revisie: 1.0.1

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

Update Revisie 1

Het NCSC ontvangt berichten dat kwetsbaarheden in Sharepoint (CVE-2025-49704 en CVE-2025-49706) actief worden misbruikt. Er is (nog) geen publieke exploitcode bekend.

Feiten

Microsoft heeft kwetsbaarheden verholpen in diverse Office producten.

Duiding

Een kwaadwillende kan de kwetsbaarheden misbruiken om zich verhoogde rechten toe te kennen, willekeurige code uit te voeren of toegang krijgen tot gevoelige gegevens.

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

UPDATE: Het NCSC ontvangt meldingen dat de kwetsbaarheden met kenmerk CVE-2025-49704 en CVE-2025-49706 actief worden misbruikt. Deze kwetsbaarheden stellen een kwaadwillende in staat om zich voor te doen als andere gebruiker en willekeurige code uit te voeren, mogelijk met verhoogde rechten. Er is (nog) geen publieke exploitcode bekend en misbruik vindt plaats op publiek toegankelijke sharepoint-installaties. Doordat de kwetsbaarheid de aandacht heeft van onderzoekers en de (toen nog theoretische) mogelijkheid van misbruik is gedemonstreerd tijdens Pwn2Own 2025 Berlijn, verwacht het NCSC een significante toename in pogingen tot misbruik.

Voor succesvol misbruik moet de kwaadwillende het slachtoffer misleiden een malafide link te volgen, waarna de kwaadwillende onder de rechten van het slachtoffer code kan uitvoeren.

Microsoft Teams:

CVE-ID	CVSS	Impact
CVE-2025-49731	3.10	Verkrijgen van verhoogde rechten
CVE-2025-49737	7.00	Verkrijgen van verhoogde rechten

Microsoft Office:

CVE-ID	CVSS	Impact
CVE-2025-47994	7.80	Verkrijgen van verhoogde rechten
CVE-2025-49695	8.40	Uitvoeren van willekeurige code

CVE-2025-49696	8.40	Uitvoeren van willekeurige code
CVE-2025-49697	8.40	Uitvoeren van willekeurige code
CVE-2025-49699	7.00	Uitvoeren van willekeurige code
CVE-2025-49702	7.80	Uitvoeren van willekeurige code

Microsoft Office Word:

CVE-ID	CVSS	Impact
CVE-2025-49698	7.80	Uitvoeren van willekeurige code
CVE-2025-49700	7.80	Uitvoeren van willekeurige code
CVE-2025-49703	7.80	Uitvoeren van willekeurige code

Microsoft Office PowerPoint:

CVE-ID	CVSS	Impact
CVE-2025-49705	7.80	Uitvoeren van willekeurige code

Microsoft Office SharePoint:

CVE-ID	CVSS	Impact
CVE-2025-49701	8.80	Uitvoeren van willekeurige code
CVE-2025-49704	8.80	Uitvoeren van willekeurige code
CVE-2025-49706	6.30	Voordoen als andere gebruiker

Microsoft Office Excel:

CVE-ID	CVSS	Impact
CVE-2025-48812	5.50	Toegang tot gevoelige gegevens
CVE-2025-49711	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>

Voor de kwetsbaarheden in Sharepoint (kenmerken CVE-2025-49704 en CVE-2025-49706) hebben onderzoekers (gedeeltelijke) Indicators of Compromise (IoC's) vrijgegeven, waarmee systeemeigenaren kunnen verifiëren of systemen geraakt zijn. Zie bijgevoegde referenties voor meer informatie.

Referenties

➤ <https://research.eye.security/sharepoint-under-siege/>

Kwetsbaarheden

CVE	CVSS Score
➤ CVE-2025-47994	
➤ CVE-2025-48812	5.5 MEDIUM
➤ CVE-2025-49711	7.8 HIGH
➤ CVE-2025-49695	8.4 HIGH
➤ CVE-2025-49696	8.4 HIGH
➤ CVE-2025-49697	8.4 HIGH
➤ CVE-2025-49698	7.8 HIGH
➤ CVE-2025-49699	7.0 HIGH
➤ CVE-2025-49700	7.8 HIGH
➤ CVE-2025-49702	7.8 HIGH
➤ CVE-2025-49703	7.8 HIGH
➤ CVE-2025-49705	7.8 HIGH

> CVE-2025-49731	3.1 LOW
> CVE-2025-49701	8.8 HIGH
> CVE-2025-49704	8.8 HIGH
> CVE-2025-49706	6.3 MEDIUM
> CVE-2025-49737	7.0 HIGH

CWE's

CWE	Beschrijving
> CVE-280	Improper Handling of Insufficient Permissions or Privileges
> CVE-843	Access of Resource Using Incompatible Type ('Type Confusion')
> CVE-285	Improper Authorization
> CVE-362	Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')
> CVE-125	Out-of-bounds Read
> CVE-416	Use After Free
> CVE-94	Improper Control of Generation of Code ('Code Injection')
> CVE-502	Deserialization of Untrusted Data
> CVE-122	Heap-based Buffer Overflow
> CVE-287	Improper Authentication

Getroffen producten

Microsoft
Microsoft Office 2019
Microsoft Office LTSC 2021

Microsoft Office LTSC 2024
Microsoft Office LTSC for Mac 2021
Microsoft Office LTSC for Mac 2024
Microsoft Office for Android
Microsoft Outlook 2016
Microsoft PowerPoint 2016
Microsoft SharePoint Enterprise Server 2016
Microsoft SharePoint Server 2019
Microsoft SharePoint Server Subscription Edition
Microsoft Teams for Android
Microsoft Teams for Desktop
Microsoft Teams for Mac
Microsoft Teams for iOS
Microsoft Word 2016
Office Online Server
Microsoft 365 Apps for Enterprise

Microsoft Excel
2016

Microsoft Office
2016

Disclaimer

The Netherlands Cyber Security Center (henceforth: NCSC-NL) maintains this page to enhance access to its information and security advisories. The use of this security advisory is subject to the following terms and conditions: NCSC-NL makes every reasonable effort to ensure that the content of this page is kept up to date, and that it is accurate and complete. Nevertheless, NCSC-NL cannot entirely rule out the possibility of errors, and therefore cannot give any warranty in respect of its completeness, accuracy or continuous keeping up-to-date. The information contained in this security advisory is intended solely for the purpose of providing general information to professional users. No rights can be derived from the information provided therein. NCSC-NL and the Kingdom of the Netherlands assume no legal liability or responsibility for any damage resulting from either the use or inability of use of this security advisory. This includes damage resulting from the inaccuracy or incompleteness of the information contained in the advisory. This security advisory is subject to Dutch law. All disputes related to or arising from the use of this advisory will be submitted to the competent court in The Hague. This choice of means also applies to the court in summary proceedings.