



# NCSC-2025-0012

## Kwetsbaarheden verholpen in Microsoft Office

NCSC Advisory

Prioriteit: Normaal

Gepubliceerd op: 14-01-2025

**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](http://www.first.org/tlp)).

Ontvangers van TLP:WHITE mogen de informatie publiek verspreiden.

Uw reacties zijn welkom op [info@ncsc.nl](mailto:info@ncsc.nl)

## Feiten

Microsoft heeft kwetsbaarheden verholpen in diverse Office producten.

## Duiding

Een kwaadwillende kan de kwetsbaarheden misbruiken om een beveiligingsmaatregel te omzeilen, zich voor te doen als andere gebruiker, toegang te krijgen tot gevoelige gegevens of willekeurige code uit te voeren in de context van het slachtoffer.

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

### Microsoft Purview:

CVE-ID	CVSS	Impact
CVE-2025-21385	8.80	Toegang tot gevoelige gegevens

### Microsoft Office Word:

CVE-ID	CVSS	Impact
CVE-2025-21363	7.80	Uitvoeren van willekeurige code

### Windows Win32K - GRFX:

CVE-ID	CVSS	Impact
CVE-2025-21338	7.80	Uitvoeren van willekeurige code

### Microsoft Office:

CVE-ID	CVSS	Impact
CVE-2025-21346	7.10	Omzeilen van beveiligingsmaatregel
CVE-2025-21365	7.80	Uitvoeren van willekeurige code

Microsoft Office Excel:

CVE-ID	CVSS	Impact
CVE-2025-21354	7.80	Uitvoeren van willekeurige code
CVE-2025-21362	7.80	Uitvoeren van willekeurige code
CVE-2025-21364	7.80	Omzeilen van beveiligingsmaatregel

Microsoft Office Outlook:

CVE-ID	CVSS	Impact
CVE-2025-21357	6.70	Uitvoeren van willekeurige code

Microsoft AutoUpdate (MAU):

CVE-ID	CVSS	Impact
CVE-2025-21360	7.80	Verkrijgen van verhoogde rechten

Microsoft Office Outlook for Mac:

CVE-ID	CVSS	Impact
CVE-2025-21361	7.80	Uitvoeren van willekeurige code

Microsoft Office Visio:

CVE-ID	CVSS	Impact
CVE-2025-21345	7.80	Uitvoeren van willekeurige code
CVE-2025-21356	7.80	Uitvoeren van willekeurige code

Microsoft Office Access:

CVE-ID	CVSS	Impact
--------	------	--------

CVE-ID	CVSS	Impact
CVE-2025-21366	7.80	Uitvoeren van willekeurige code
CVE-2025-21395	7.80	Uitvoeren van willekeurige code
CVE-2025-21186	7.80	Uitvoeren van willekeurige code

Microsoft Office OneNote:

CVE-ID	CVSS	Impact
CVE-2025-21402	7.80	Uitvoeren van willekeurige code

Microsoft Office SharePoint:

CVE-ID	CVSS	Impact
CVE-2025-21344	7.80	Uitvoeren van willekeurige code
CVE-2025-21348	7.20	Uitvoeren van willekeurige code
CVE-2025-21393	6.30	Voordoen als andere gebruiker

## 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>

## Kwetsbaarheden

CVE	CVSS Score
> CVE-2025-21186	7.8 HIGH
> CVE-2025-21338	7.8 HIGH
> CVE-2025-21344	7.8 HIGH

> CVE-2025-21345	7.8 HIGH
> CVE-2025-21346	7.1 HIGH
> CVE-2025-21348	7.2 HIGH
> CVE-2025-21354	7.8 HIGH
> CVE-2025-21356	7.8 HIGH
> CVE-2025-21357	6.7 MEDIUM
> CVE-2025-21360	7.8 HIGH
> CVE-2025-21361	7.8 HIGH
> CVE-2025-21362	7.8 HIGH
> CVE-2025-21363	7.8 HIGH
> CVE-2025-21364	7.8 HIGH
> CVE-2025-21365	7.8 HIGH
> CVE-2025-21366	7.8 HIGH
> CVE-2025-21385	8.8 HIGH
> CVE-2025-21393	6.3 MEDIUM
> CVE-2025-21395	7.8 HIGH
> CVE-2025-21402	7.8 HIGH

## CWE's

CWE	Beschrijving
> CVE-641	Improper Restriction of Names for Files and Other Resources
> CVE-822	Untrusted Pointer Dereference
> CVE-908	Use of Uninitialized Resource
> CVE-426	Untrusted Search Path

› CWE-843	Access of Resource Using Incompatible Type ('Type Confusion')
› CWE-190	Integer Overflow or Wraparound
› CWE-693	Protection Mechanism Failure
› CWE-285	Improper Authorization
› CWE-416	Use After Free
› CWE-502	Deserialization of Untrusted Data
› CWE-122	Heap-based Buffer Overflow
› CWE-269	Improper Privilege Management
› CWE-20	Improper Input Validation
› CWE-79	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')

## Getroffen producten

<b>microsoft</b>
microsoft_365_apps_for_enterprise
microsoft_access_2016
microsoft_access_2016__32-bit_edition_
microsoft_autoupdate_for_mac
microsoft_excel_2016
microsoft_office_2016
microsoft_office_2019
microsoft_office_for_android
microsoft_office_for_ios
microsoft_office_for_mac
microsoft_office_for_universal

microsoft_office_ltsc_2021
microsoft_office_ltsc_2024
microsoft_office_ltsc_for_mac_2021
microsoft_office_ltsc_for_mac_2024
microsoft_onenote
microsoft_outlook_2016
microsoft_outlook_for_mac
microsoft_purview
microsoft_sharepoint_enterprise_server_2016
microsoft_sharepoint_server_2019
microsoft_sharepoint_server_subscription_edition
office_online_server
office_purview
purview

## 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.