



# NCSC-2024-0337

## Kwetsbaarheden verholpen in Microsoft Office

NCSC Advisory

Prioriteit: Normaal

Gepubliceerd op: 13-08-2024

### **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 zich voor te doen als andere gebruiker, willekeurige code uit te voeren met rechten van het slachtoffer en mogelijk toegang te krijgen tot gevoelige gegevens 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 Teams:

CVE-ID	CVSS	Impact
CVE-2024-38197	6.50	Voordoen als andere gebruiker

### Microsoft Office:

CVE-ID	CVSS	Impact
CVE-2024-38084	7.80	Verkrijgen van verhoogde rechten
CVE-2024-38200	7.50	Voordoen als andere gebruiker

### Microsoft Office Outlook:

CVE-ID	CVSS	Impact
CVE-2024-38173	6.70	Uitvoeren van willekeurige code

### Microsoft Office Visio:

CVE-ID	CVSS	Impact
CVE-2024-38169	7.80	Uitvoeren van willekeurige code

Microsoft Office Project:

CVE-ID	CVSS	Impact
CVE-2024-38189	8.80	Uitvoeren van willekeurige code

Microsoft Office PowerPoint:

CVE-ID	CVSS	Impact
CVE-2024-38171	7.80	Uitvoeren van willekeurige code

Microsoft Copilot Studio:

CVE-ID	CVSS	Impact
CVE-2024-38206	8.50	Toegang tot gevoelige gegevens

Microsoft Office Excel:

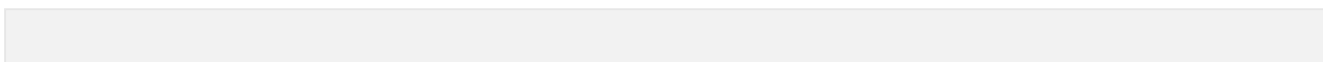
CVE-ID	CVSS	Impact
CVE-2024-38172	7.80	Uitvoeren van willekeurige code
CVE-2024-38170	7.10	Uitvoeren van willekeurige code

## 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>

## Kwetsbaarheden



CVE	CVSS Score
> CVE-2024-38172	7.8 HIGH
> CVE-2024-38169	7.8 HIGH
> CVE-2024-38170	7.1 HIGH
> CVE-2024-38171	7.8 HIGH
> CVE-2024-38173	6.7 MEDIUM
> CVE-2024-38189	8.8 HIGH
> CVE-2024-38200	9.1 CRITICAL
> CVE-2024-38197	6.5 MEDIUM
> CVE-2024-38084	7.8 HIGH
> CVE-2024-38206	8.5 HIGH

## CWE's

CWE	Beschrijving
> CWE-122	Heap-based Buffer Overflow
> CWE-20	Improper Input Validation
> CWE-200	Exposure of Sensitive Information to an Unauthorized Actor
> CWE-416	Use After Free
> CWE-451	User Interface (UI) Misrepresentation of Critical Information
> CWE-59	Improper Link Resolution Before File Access ('Link Following')
> CWE-73	External Control of File Name or Path
> CWE-918	Server-Side Request Forgery (SSRF)

## Getroffen producten

<b>microsoft</b>
365_apps
copilot_studio
microsoft_365_apps_for_enterprise
microsoft_copilot_studio
microsoft_office_2016
microsoft_office_2019
microsoft_office_ltsc_2021
microsoft_office_ltsc_for_mac_2021
microsoft_officeplus
microsoft_outlook_2016
microsoft_powerpoint_2016
microsoft_project_2016
microsoft_teams_for_ios
office_2016
office_2019
office_long_term_servicing_channel
office
outlook

## 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 of 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.