



# NCSC-2025-0155

## Kwetsbaarheden verholpen in Microsoft Office

NCSC Advisory

Prioriteit: Normaal

Gepubliceerd op: 13-05-2025

**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 zich verhoogde rechten toe te kennen en willekeurige code uit te voeren met rechten van het slachtoffer.

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

Microsoft Office PowerPoint:

| CVE-ID         | CVSS | Impact                          |
|----------------|------|---------------------------------|
| CVE-2025-29978 | 7.80 | Uitvoeren van willekeurige code |

Microsoft Office Outlook:

| CVE-ID         | CVSS | Impact                          |
|----------------|------|---------------------------------|
| CVE-2025-32705 | 7.80 | Uitvoeren van willekeurige code |

Microsoft Office:

| CVE-ID         | CVSS | Impact                          |
|----------------|------|---------------------------------|
| CVE-2025-30377 | 8.40 | Uitvoeren van willekeurige code |
| CVE-2025-30386 | 8.40 | Uitvoeren van willekeurige code |

Microsoft Office SharePoint:

| CVE-ID         | CVSS | Impact                           |
|----------------|------|----------------------------------|
| CVE-2025-29976 | 7.80 | Verkrijgen van verhoogde rechten |
| CVE-2025-30378 | 7.00 | Uitvoeren van willekeurige code  |
| CVE-2025-30382 | 7.80 | Uitvoeren van willekeurige code  |

|                |      |                                 |
|----------------|------|---------------------------------|
| CVE-2025-30384 | 7.40 | Uitvoeren van willekeurige code |
|----------------|------|---------------------------------|

Microsoft Office Excel:

| CVE-ID         | CVSS | Impact                          |
|----------------|------|---------------------------------|
| CVE-2025-29977 | 7.80 | Uitvoeren van willekeurige code |
| CVE-2025-29979 | 7.80 | Uitvoeren van willekeurige code |
| CVE-2025-30375 | 7.80 | Uitvoeren van willekeurige code |
| CVE-2025-30376 | 7.80 | Uitvoeren van willekeurige code |
| CVE-2025-30379 | 7.80 | Uitvoeren van willekeurige code |
| CVE-2025-30381 | 7.80 | Uitvoeren van willekeurige code |
| CVE-2025-30383 | 7.80 | Uitvoeren van willekeurige code |
| CVE-2025-30393 | 7.80 | Uitvoeren van willekeurige code |
| CVE-2025-32704 | 8.40 | Uitvoeren van willekeurige code |

Windows Win32K - GRFX:

| CVE-ID         | CVSS | Impact                          |
|----------------|------|---------------------------------|
| CVE-2025-30388 | 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>

## Kwetsbaarheden

| CVE                                 | CVSS Score      |
|-------------------------------------|-----------------|
| <a href="#">&gt; CVE-2025-29976</a> |                 |
| <a href="#">&gt; CVE-2025-30378</a> | <b>7.0 HIGH</b> |

|                  |          |
|------------------|----------|
| > CVE-2025-30382 |          |
| > CVE-2025-30384 |          |
| > CVE-2025-29977 |          |
| > CVE-2025-29979 | 7.8 HIGH |
| > CVE-2025-30375 |          |
| > CVE-2025-30376 | 7.8 HIGH |
| > CVE-2025-30379 |          |
| > CVE-2025-30381 |          |
| > CVE-2025-30383 | 7.8 HIGH |
| > CVE-2025-30377 |          |
| > CVE-2025-30386 | 8.4 HIGH |
| > CVE-2025-32704 |          |
| > CVE-2025-29978 |          |
| > CVE-2025-30393 | 7.8 HIGH |
| > CVE-2025-32705 |          |
| > CVE-2025-30388 | 7.8 HIGH |

## CWE's

| CWE       | Beschrijving  |
|-----------|---|
| > CVE-763 | Release of Invalid Pointer or Reference                       |
| > CVE-822 | Untrusted Pointer Dereference                                 |
| > CVE-126 | Buffer Over-read  |
| > CVE-843 | Access of Resource Using Incompatible Type ('Type Confusion') |
| > CVE-125 | Out-of-bounds Read  |

|           |                                   |
|-----------|-----------------------------------|
| ➤ CWE-416 | Use After Free                    |
| ➤ CWE-502 | Deserialization of Untrusted Data |
| ➤ CWE-122 | Heap-based Buffer Overflow        |
| ➤ CWE-269 | Improper Privilege Management     |

## Getroffen producten

|  |
|--|
| <b>Microsoft</b>                               |
| 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 LTSC for Mac 2021             |
| Microsoft Office LTSC for Mac 2024             |
| Microsoft Office LTSC 2021 for 32-bit editions |
| Microsoft Office LTSC 2024 for 32-bit editions |
| Microsoft Office LTSC 2024 for 64-bit editions |

|   |
|---|
| Microsoft SharePoint Server<br>Subscription Edition     |
| Microsoft SharePoint<br>Server 2019                     |
| Microsoft SharePoint Enterprise<br>Server 2016          |
| Microsoft 365 Apps for Enterprise<br>for 32-bit Systems |
| Microsoft 365 Apps for Enterprise<br>for 64-bit Systems |
| Office  |
| powerpoint  |
| sharepoint_server                                       |

## 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.