



## Advisory NCSC-2026-0422

PRIORITEIT: NORMAAL

# Kwetsbaarheden verholpen in Microsoft Office

Publicatiedatum: 13-10-2026

Toegestane verspreiding: TLP:WHITE  
(Traffic Light Protocol)

Deze publicatie bevat het label TLP:WHITE en wordt door het Nationaal Cyber Security Center (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.

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

## Feiten

Microsoft heeft xxx kwetsbaarheden verholpen in diverse Office producten, zoals Word, Excel, Access, Outlook, Visio, Sharepoint en PowerPoint, maar ook subcomponenten als Shell, Azure Key Vault en Click-to-Run.

## Duiding

Een kwaadwillende kan de kwetsbaarheden misbruiken om een Denial-of-Service te veroorzaken, zich verhoogde rechten toe te kennen, willekeurige code uit te voeren en toegang te krijgen tot gevoelige informatie in de context van het slachtoffer.

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

Van de kwetsbaarheid met kenmerk CVE-2026-96951 meldt Microsoft bekend te zijn met het feit dat deze beperkt en gericht is misbruikt. Er is geen Proof-of-Concept-code (PoC) of exploit bekend en succesvol misbruik vereist social engineering.

Microsoft Office Click-To-Run: |-----|---|-----|

| CVE-ID         | CVSS | Impact                           |
|----------------|------|----------------------------------|
| CVE-2026-70276 | 7.00 | Verkrijgen van verhoogde rechten |
| CVE-2026-85340 | 7.80 | Verkrijgen van verhoogde rechten |
| -----          | ---  | -----                            |

Microsoft Office SharePoint: |-----|---|-----|

| CVE-ID          | CVSS | Impact                           |
|-----------------|------|----------------------------------|
| CVE-2026-102859 | 4.60 | Voordoen als andere gebruiker    |
| CVE-2026-102860 | 8.80 | Verkrijgen van verhoogde rechten |
| CVE-2026-102861 | 8.80 | Verkrijgen van verhoogde rechten |
| CVE-2026-102862 | 8.80 | Verkrijgen van verhoogde rechten |
| CVE-2026-102863 | 8.80 | Verkrijgen van verhoogde rechten |
| CVE-2026-102864 | 4.60 | Voordoen als andere gebruiker    |
| CVE-2026-102865 | 6.50 | Toegang tot gevoelige gegevens   |
| CVE-2026-102866 | 8.10 | Verkrijgen van verhoogde rechten |
| CVE-2026-105013 | 7.40 | Uitvoeren van willekeurige code  |
| CVE-2026-105713 | 5.70 | Voordoen als andere gebruiker    |
| CVE-2026-105719 | 6.50 | Toegang tot gevoelige gegevens   |
| CVE-2026-105720 | 4.30 | Verkrijgen van verhoogde rechten |
| CVE-2026-69943  | 8.80 | Uitvoeren van willekeurige code  |
| CVE-2026-70202  | 7.50 | Verkrijgen van verhoogde rechten |
| CVE-2026-70217  | 4.90 | Toegang tot gevoelige gegevens   |
| CVE-2026-70246  | 8.80 | Verkrijgen van verhoogde rechten |
| CVE-2026-70251  | 7.50 | Verkrijgen van verhoogde rechten |
| CVE-2026-70259  | 6.50 | Toegang tot gevoelige gegevens   |
| CVE-2026-70266  | 8.80 | Verkrijgen van verhoogde rechten |
| CVE-2026-70267  | 7.20 | Uitvoeren van willekeurige code  |
| CVE-2026-70298  | 6.50 | Toegang tot gevoelige gegevens   |
| CVE-2026-85900  | 8.80 | Uitvoeren van willekeurige code  |
| CVE-2026-85932  | 6.50 | Toegang tot gevoelige gegevens   |
| CVE-2026-88155  | 8.80 | Uitvoeren van willekeurige code  |
| CVE-2026-88163  | 8.80 | <Vertaal: Not a Vulnerability>   |
| CVE-2026-88166  | 8.80 | Uitvoeren van willekeurige code  |
| CVE-2026-88198  | 8.80 | Verkrijgen van verhoogde rechten |
| CVE-2026-88200  | 8.80 | Verkrijgen van verhoogde rechten |
| CVE-2026-88204  | 7.30 | Voordoen als andere gebruiker    |
| CVE-2026-88206  | 7.50 | Verkrijgen van verhoogde rechten |
| CVE-2026-88208  | 4.60 | Voordoen als andere gebruiker    |
| CVE-2026-88209  | 4.60 | Voordoen als andere gebruiker    |
| CVE-2026-96044  | 8.80 | Verkrijgen van verhoogde rechten |
| CVE-2026-97782  | 6.80 | <Vertaal: Tampering>             |
| CVE-2026-97783  | 8.10 | Voordoen als andere gebruiker    |

Windows Rich Text Edit Control: |-----|-----|-----|

| CVE-ID         | CVSS | Impact                          |
|----------------|------|---------------------------------|
| CVE-2026-70096 | 9.80 | Uitvoeren van willekeurige code |

Microsoft Office Excel: |-----|-----|-----|

| CVE-ID          | CVSS | Impact                          |
|-----------------|------|---------------------------------|
| CVE-2026-100209 | 8.80 | Uitvoeren van willekeurige code |
| CVE-2026-100210 | 8.80 | Uitvoeren van willekeurige code |
| CVE-2026-100211 | 8.80 | Uitvoeren van willekeurige code |
| CVE-2026-100212 | 8.80 | Uitvoeren van willekeurige code |
| CVE-2026-105718 | 8.80 | Uitvoeren van willekeurige code |
| CVE-2026-70214  | 5.50 | Toegang tot gevoelige gegevens  |
| CVE-2026-70219  | 6.50 | Toegang tot gevoelige gegevens  |
| CVE-2026-70254  | 8.80 | Uitvoeren van willekeurige code |
| CVE-2026-77902  | 8.80 | Uitvoeren van willekeurige code |
| CVE-2026-88145  | 8.80 | Uitvoeren van willekeurige code |
| CVE-2026-88151  | 6.50 | Toegang tot gevoelige gegevens  |
| CVE-2026-88153  | 6.50 | Toegang tot gevoelige gegevens  |
| CVE-2026-88154  | 6.50 | Toegang tot gevoelige gegevens  |
| CVE-2026-88172  | 6.50 | Toegang tot gevoelige gegevens  |
| CVE-2026-88175  | 6.50 | Toegang tot gevoelige gegevens  |
| CVE-2026-88184  | 6.50 | Toegang tot gevoelige gegevens  |
| CVE-2026-88190  | 6.50 | Toegang tot gevoelige gegevens  |
| CVE-2026-88192  | 6.50 | Toegang tot gevoelige gegevens  |
| CVE-2026-88195  | 6.50 | Toegang tot gevoelige gegevens  |
| CVE-2026-88201  | 6.50 | Toegang tot gevoelige gegevens  |
| CVE-2026-97003  | 8.80 | Uitvoeren van willekeurige code |
| CVE-2026-97004  | 8.80 | Uitvoeren van willekeurige code |
| CVE-2026-97007  | 8.80 | Uitvoeren van willekeurige code |
| CVE-2026-97008  | 8.80 | Uitvoeren van willekeurige code |
| CVE-2026-97009  | 7.80 | Uitvoeren van willekeurige code |
| CVE-2026-97010  | 8.80 | Uitvoeren van willekeurige code |
| CVE-2026-97011  | 8.80 | Uitvoeren van willekeurige code |
| CVE-2026-97014  | 5.50 | Toegang tot gevoelige gegevens  |
| CVE-2026-97017  | 8.80 | Uitvoeren van willekeurige code |
| CVE-2026-97738  | 8.80 | Uitvoeren van willekeurige code |
| CVE-2026-97739  | 8.80 | Uitvoeren van willekeurige code |
| CVE-2026-97740  | 6.50 | Toegang tot gevoelige gegevens  |
| CVE-2026-97741  | 8.80 | Uitvoeren van willekeurige code |
| CVE-2026-97742  | 8.80 | Uitvoeren van willekeurige code |
| CVE-2026-97743  | 6.50 | Toegang tot gevoelige gegevens  |
| CVE-2026-97745  | 8.80 | Uitvoeren van willekeurige code |
| CVE-2026-97746  | 8.80 | Uitvoeren van willekeurige code |
| CVE-2026-97747  | 8.80 | Uitvoeren van willekeurige code |
| CVE-2026-97748  | 8.80 | Uitvoeren van willekeurige code |
| CVE-2026-97750  | 8.80 | Uitvoeren van willekeurige code |
| CVE-2026-97751  | 8.80 | Uitvoeren van willekeurige code |
| CVE-2026-97752  | 8.80 | Uitvoeren van willekeurige code |
| CVE-2026-97753  | 8.80 | Uitvoeren van willekeurige code |
| CVE-2026-97754  | 8.80 | Uitvoeren van willekeurige code |
| CVE-2026-97755  | 8.80 | Uitvoeren van willekeurige code |
| CVE-2026-97756  | 8.80 | Uitvoeren van willekeurige code |
| CVE-2026-97757  | 8.80 | Uitvoeren van willekeurige code |
| CVE-2026-97758  | 8.80 | Uitvoeren van willekeurige code |
| CVE-2026-97759  | 8.80 | Uitvoeren van willekeurige code |
| CVE-2026-97760  | 6.50 | Toegang tot gevoelige gegevens  |
| CVE-2026-97761  | 8.80 | Uitvoeren van willekeurige code |
| CVE-2026-97762  | 8.80 | Uitvoeren van willekeurige code |
| CVE-2026-97763  | 8.80 | Uitvoeren van willekeurige code |

Windows Shell: |-----|-----|-----|

| CVE-ID         | CVSS | Impact                             |
|----------------|------|------------------------------------|
| CVE-2026-96951 | 8.80 | Omzeilen van beveiligingsmaatregel |

Microsoft Office Word: |-----|-----|-----|

| CVE-ID          | CVSS | Impact                             |
|-----------------|------|------------------------------------|
| CVE-2026-102867 | 6.50 | Denial-of-Service                  |
| CVE-2026-105715 | 7.50 | Uitvoeren van willekeurige code    |
| CVE-2026-70206  | 6.50 | Toegang tot gevoelige gegevens     |
| CVE-2026-70220  | 7.80 | Uitvoeren van willekeurige code    |
| CVE-2026-70263  | 6.50 | Toegang tot gevoelige gegevens     |
| CVE-2026-70268  | 8.80 | Uitvoeren van willekeurige code    |
| CVE-2026-70269  | 8.10 | Uitvoeren van willekeurige code    |
| CVE-2026-70287  | 8.80 | Uitvoeren van willekeurige code    |
| CVE-2026-70300  | 9.80 | Uitvoeren van willekeurige code    |
| CVE-2026-70301  | 8.80 | Uitvoeren van willekeurige code    |
| CVE-2026-70302  | 8.80 | Uitvoeren van willekeurige code    |
| CVE-2026-83891  | 8.80 | Uitvoeren van willekeurige code    |
| CVE-2026-88150  | 8.80 | Uitvoeren van willekeurige code    |
| CVE-2026-88167  | 6.50 | Toegang tot gevoelige gegevens     |
| CVE-2026-88169  | 6.50 | Toegang tot gevoelige gegevens     |
| CVE-2026-88185  | 8.10 | Uitvoeren van willekeurige code    |
| CVE-2026-88186  | 8.80 | Uitvoeren van willekeurige code    |
| CVE-2026-88202  | 8.80 | Uitvoeren van willekeurige code    |
| CVE-2026-88210  | 7.80 | Omzeilen van beveiligingsmaatregel |
| CVE-2026-96995  | 7.80 | Verkrijgen van verhoogde rechten   |
| CVE-2026-96996  | 7.80 | Uitvoeren van willekeurige code    |
| CVE-2026-97001  | 7.80 | Uitvoeren van willekeurige code    |

Microsoft Office: |-----|-----|-----|

| CVE-ID         | CVSS | Impact                          |
|----------------|------|---------------------------------|
| CVE-2026-88196 | 8.80 | Uitvoeren van willekeurige code |
| CVE-2026-88197 | 8.80 | Uitvoeren van willekeurige code |

Microsoft Office Visio: |-----|-----|-----|

| CVE-ID          | CVSS | Impact                          |
|-----------------|------|---------------------------------|
| CVE-2026-102855 | 8.80 | Uitvoeren van willekeurige code |
| CVE-2026-102856 | 8.80 | Uitvoeren van willekeurige code |
| CVE-2026-102857 | 8.80 | Uitvoeren van willekeurige code |

Microsoft Office Outlook: |-----|-----|-----|

| CVE-ID         | CVSS | Impact                          |
|----------------|------|---------------------------------|
| CVE-2026-70242 | 9.80 | Uitvoeren van willekeurige code |
| CVE-2026-70256 | 8.80 | Uitvoeren van willekeurige code |
| CVE-2026-70257 | 8.80 | Uitvoeren van willekeurige code |
| CVE-2026-70281 | 7.50 | Toegang tot gevoelige gegevens  |
| CVE-2026-70282 | 8.80 | Uitvoeren van willekeurige code |
| CVE-2026-70291 | 9.80 | Uitvoeren van willekeurige code |
| CVE-2026-88156 | 9.80 | Uitvoeren van willekeurige code |
| CVE-2026-97012 | 8.80 | Uitvoeren van willekeurige code |
| CVE-2026-97016 | 9.80 | Uitvoeren van willekeurige code |
| CVE-2026-97749 | 9.80 | Uitvoeren van willekeurige code |

Microsoft Office OneNote: |-----|-----|-----|

| CVE-ID         | CVSS | Impact                           |
|----------------|------|----------------------------------|
| CVE-2026-96997 | 7.80 | Verkrijgen van verhoogde rechten |

Microsoft Office PowerPoint: |-----|-----|-----|

| CVE-ID          | CVSS | Impact                          |
|-----------------|------|---------------------------------|
| CVE-2026-105599 | 7.50 | Uitvoeren van willekeurige code |
| CVE-2026-70215  | 8.80 | Uitvoeren van willekeurige code |
| CVE-2026-88144  | 8.80 | Uitvoeren van willekeurige code |
| CVE-2026-88178  | 9.80 | Uitvoeren van willekeurige code |
| CVE-2026-88183  | 6.50 | Toegang tot gevoelige gegevens  |
| CVE-2026-88203  | 6.50 | Toegang tot gevoelige gegevens  |
| CVE-2026-88207  | 7.50 | Uitvoeren van willekeurige code |
| CVE-2026-97005  | 5.50 | Toegang tot gevoelige gegevens  |
| CVE-2026-97744  | 5.50 | Toegang tot gevoelige gegevens  |

Microsoft Office Access: |-----|-----|-----|

| CVE-ID          | CVSS | Impact                          |
|-----------------|------|---------------------------------|
| CVE-2026-102849 | 8.80 | Uitvoeren van willekeurige code |
| CVE-2026-102850 | 8.80 | Uitvoeren van willekeurige code |
| CVE-2026-105591 | 8.80 | Uitvoeren van willekeurige code |
| CVE-2026-105592 | 7.50 | Uitvoeren van willekeurige code |
| CVE-2026-105593 | 8.80 | Uitvoeren van willekeurige code |
| CVE-2026-105595 | 8.80 | Uitvoeren van willekeurige code |
| CVE-2026-105596 | 8.80 | Uitvoeren van willekeurige code |
| CVE-2026-105597 | 8.80 | Uitvoeren van willekeurige code |
| CVE-2026-105598 | 8.80 | Uitvoeren van willekeurige code |
| CVE-2026-105714 | 7.50 | Uitvoeren van willekeurige code |
| CVE-2026-105716 | 8.80 | Uitvoeren van willekeurige code |
| CVE-2026-105717 | 8.80 | Uitvoeren van willekeurige code |
| CVE-2026-94506  | 6.50 | Toegang tot gevoelige gegevens  |

Azure Key Vault: |-----|-----|-----|

| CVE-ID         | CVSS | Impact                             |
|----------------|------|------------------------------------|
| CVE-2026-85922 | 7.40 | Omzeilen van beveiligingsmaatregel |
| CVE-2026-85925 | 8.20 | Verkrijgen van verhoogde rechten   |
| CVE-2026-88132 | 5.90 | Toegang tot gevoelige gegevens     |

Skype for Business and Microsoft Lync: |-----|-----|-----|

| CVE-ID         | CVSS | Impact                           |
|----------------|------|----------------------------------|
| CVE-2026-70297 | 8.80 | Uitvoeren van willekeurige code  |
| CVE-2026-83746 | 8.10 | Verkrijgen van verhoogde rechten |
| CVE-2026-85873 | 6.50 | Verkrijgen van verhoogde rechten |

Azure DevOps: |-----|-----|-----|

| CVE-ID         | CVSS | Impact                         |
|----------------|------|--------------------------------|
| CVE-2026-69877 | 6.50 | Toegang tot gevoelige gegevens |

## 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-2026-100209 |            |
| CVE-2026-100210 |            |
| CVE-2026-100211 |            |
| CVE-2026-100212 |            |
| CVE-2026-102849 |            |
| CVE-2026-102850 |            |
| CVE-2026-102855 |            |
| CVE-2026-102856 |            |
| CVE-2026-102857 |            |
| CVE-2026-102859 |            |

| CVE             | CVSS Score |
|-----------------|------------|
| CVE-2026-102860 |            |
| CVE-2026-102861 |            |
| CVE-2026-102862 |            |
| CVE-2026-102863 |            |
| CVE-2026-102864 |            |
| CVE-2026-102865 |            |
| CVE-2026-102866 |            |
| CVE-2026-102867 |            |
| CVE-2026-105013 |            |
| CVE-2026-105591 |            |
| CVE-2026-105592 |            |
| CVE-2026-105593 |            |
| CVE-2026-105595 |            |
| CVE-2026-105596 |            |
| CVE-2026-105597 |            |
| CVE-2026-105598 |            |
| CVE-2026-105599 |            |
| CVE-2026-105713 |            |
| CVE-2026-105714 |            |
| CVE-2026-105715 |            |
| CVE-2026-105716 |            |
| CVE-2026-105717 |            |
| CVE-2026-105718 |            |
| CVE-2026-105719 |            |
| CVE-2026-105720 |            |
| CVE-2026-69877  |            |
| CVE-2026-69943  |            |
| CVE-2026-70096  |            |
| CVE-2026-70202  |            |
| CVE-2026-70206  |            |
| CVE-2026-70214  |            |
| CVE-2026-70215  |            |

| CVE            | CVSS Score |
|----------------|------------|
| CVE-2026-70217 |            |
| CVE-2026-70219 |            |
| CVE-2026-70220 |            |
| CVE-2026-70242 |            |
| CVE-2026-70246 |            |
| CVE-2026-70251 |            |
| CVE-2026-70254 |            |
| CVE-2026-70256 |            |
| CVE-2026-70257 |            |
| CVE-2026-70259 |            |
| CVE-2026-70263 |            |
| CVE-2026-70266 |            |
| CVE-2026-70267 |            |
| CVE-2026-70268 |            |
| CVE-2026-70269 |            |
| CVE-2026-70276 |            |
| CVE-2026-70281 |            |
| CVE-2026-70282 |            |
| CVE-2026-70287 |            |
| CVE-2026-70291 |            |
| CVE-2026-70297 |            |
| CVE-2026-70298 |            |
| CVE-2026-70300 |            |
| CVE-2026-70301 |            |
| CVE-2026-70302 |            |
| CVE-2026-77902 |            |
| CVE-2026-83746 |            |
| CVE-2026-83891 |            |
| CVE-2026-85340 |            |
| CVE-2026-85873 |            |
| CVE-2026-85900 |            |
| CVE-2026-85922 |            |

| CVE            | CVSS Score |
|----------------|------------|
| CVE-2026-85925 |            |
| CVE-2026-85932 |            |
| CVE-2026-88132 |            |
| CVE-2026-88144 |            |
| CVE-2026-88145 |            |
| CVE-2026-88150 |            |
| CVE-2026-88151 |            |
| CVE-2026-88153 |            |
| CVE-2026-88154 |            |
| CVE-2026-88155 |            |
| CVE-2026-88156 |            |
| CVE-2026-88163 |            |
| CVE-2026-88166 |            |
| CVE-2026-88167 |            |
| CVE-2026-88169 |            |
| CVE-2026-88172 |            |
| CVE-2026-88175 |            |
| CVE-2026-88178 |            |
| CVE-2026-88183 |            |
| CVE-2026-88184 |            |
| CVE-2026-88185 |            |
| CVE-2026-88186 |            |
| CVE-2026-88190 |            |
| CVE-2026-88192 |            |
| CVE-2026-88195 |            |
| CVE-2026-88196 |            |
| CVE-2026-88197 |            |
| CVE-2026-88198 |            |
| CVE-2026-88200 |            |
| CVE-2026-88201 |            |
| CVE-2026-88202 |            |
| CVE-2026-88203 |            |

| CVE            | CVSS Score |
|----------------|------------|
| CVE-2026-88204 |            |
| CVE-2026-88206 |            |
| CVE-2026-88207 |            |
| CVE-2026-88208 |            |
| CVE-2026-88209 |            |
| CVE-2026-88210 |            |
| CVE-2026-94506 |            |
| CVE-2026-96044 |            |
| CVE-2026-96951 |            |
| CVE-2026-96995 |            |
| CVE-2026-96996 |            |
| CVE-2026-96997 |            |
| CVE-2026-97001 |            |
| CVE-2026-97003 |            |
| CVE-2026-97004 |            |
| CVE-2026-97005 |            |
| CVE-2026-97007 |            |
| CVE-2026-97008 |            |
| CVE-2026-97009 |            |
| CVE-2026-97010 |            |
| CVE-2026-97011 |            |
| CVE-2026-97012 |            |
| CVE-2026-97014 |            |
| CVE-2026-97016 |            |
| CVE-2026-97017 |            |
| CVE-2026-97738 |            |
| CVE-2026-97739 |            |
| CVE-2026-97740 |            |
| CVE-2026-97741 |            |
| CVE-2026-97742 |            |
| CVE-2026-97743 |            |
| CVE-2026-97744 |            |

| CVE            | CVSS Score |
|----------------|------------|
| CVE-2026-97745 |            |
| CVE-2026-97746 |            |
| CVE-2026-97747 |            |
| CVE-2026-97748 |            |
| CVE-2026-97749 |            |
| CVE-2026-97750 |            |
| CVE-2026-97751 |            |
| CVE-2026-97752 |            |
| CVE-2026-97753 |            |
| CVE-2026-97754 |            |
| CVE-2026-97755 |            |
| CVE-2026-97756 |            |
| CVE-2026-97757 |            |
| CVE-2026-97758 |            |
| CVE-2026-97759 |            |
| CVE-2026-97760 |            |
| CVE-2026-97761 |            |
| CVE-2026-97762 |            |
| CVE-2026-97763 |            |
| CVE-2026-97765 |            |
| CVE-2026-97766 |            |
| CVE-2026-97767 |            |
| CVE-2026-97768 |            |
| CVE-2026-97769 |            |
| CVE-2026-97770 |            |
| CVE-2026-97771 |            |
| CVE-2026-97772 |            |
| CVE-2026-97773 |            |
| CVE-2026-97775 |            |
| CVE-2026-97776 |            |
| CVE-2026-97777 |            |
| CVE-2026-97778 |            |

| CVE            | CVSS Score |
|----------------|------------|
| CVE-2026-97779 |            |
| CVE-2026-97780 |            |
| CVE-2026-97782 |            |
| CVE-2026-97783 |            |

## CWE's

| CWE     | Beschrijving                                                                         |
|---------|--------------------------------------------------------------------------------------|
| CWE-22  | Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')       |
| CWE-36  | Absolute Path Traversal                                                              |
| CWE-77  | Improper Neutralization of Special Elements used in a Command ('Command Injection')  |
| CWE-79  | Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') |
| CWE-89  | Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') |
| CWE-94  | Improper Control of Generation of Code ('Code Injection')                            |
| CWE-121 | Stack-based Buffer Overflow                                                          |
| CWE-122 | Heap-based Buffer Overflow                                                           |
| CWE-124 | Buffer Underwrite ('Buffer Underflow')                                               |
| CWE-125 | Out-of-bounds Read                                                                   |
| CWE-126 | Buffer Over-read                                                                     |
| CWE-190 | Integer Overflow or Wraparound                                                       |
| CWE-191 | Integer Underflow (Wrap or Wraparound)                                               |
| CWE-193 | Off-by-one Error                                                                     |
| CWE-197 | Numeric Truncation Error                                                             |
| CWE-203 | Observable Discrepancy                                                               |
| CWE-270 | Privilege Context Switching Error                                                    |
| CWE-346 | Origin Validation Error                                                              |
| CWE-347 | Improper Verification of Cryptographic Signature                                     |

| CWE      | Beschrijving                                                               |
|----------|----------------------------------------------------------------------------|
| CWE-415  | Double Free                                                                |
| CWE-416  | Use After Free                                                             |
| CWE-476  | NULL Pointer Dereference                                                   |
| CWE-497  | Exposure of Sensitive System Information to an Unauthorized Control Sphere |
| CWE-502  | Deserialization of Untrusted Data                                          |
| CWE-763  | Release of Invalid Pointer or Reference                                    |
| CWE-787  | Out-of-bounds Write                                                        |
| CWE-807  | Reliance on Untrusted Inputs in a Security Decision                        |
| CWE-822  | Untrusted Pointer Dereference                                              |
| CWE-829  | Inclusion of Functionality from Untrusted Control Sphere                   |
| CWE-862  | Missing Authorization                                                      |
| CWE-863  | Incorrect Authorization                                                    |
| CWE-908  | Use of Uninitialized Resource                                              |
| CWE-918  | Server-Side Request Forgery (SSRF)                                         |
| CWE-923  | Improper Restriction of Communication Channel to Intended Endpoints        |
| CWE-1390 | Weak Authentication                                                        |

## Getroffen producten

| Microsoft                                            |
|------------------------------------------------------|
| Microsoft 365 Apps for Enterprise for 32-bit Systems |
| Microsoft 365 Apps for Enterprise for 64-bit Systems |
| Microsoft Office 365 for Mac                         |
| Microsoft Office LTSC 2021 for 32-bit editions       |
| Microsoft Office LTSC 2021 for 64-bit editions       |
| Microsoft Office LTSC 2024 for 32-bit editions       |
| Microsoft Office LTSC 2024 for 64-bit editions       |
| Microsoft Office LTSC for Mac 2021                   |
| Microsoft Office LTSC for Mac 2024                   |

**Microsoft**

Microsoft SharePoint Enterprise Server 2016

Microsoft SharePoint Server 2019

Microsoft SharePoint Server Subscription Edition

Office Online Server

Outlook.com

Skype for Business Server 2015 CU13

Skype for Business Server 2019 CU8

Skype for Business Server Subscription Edition CU1

## 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.