



# NCSC-2026-0010

## Kwetsbaarheden verholpen in Microsoft Office

NCSC Advisory

Prioriteit: Normaal

Gepubliceerd op: 20-03-2026

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](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)

## Update Revisie 1

Er worden berichten gepubliceerd dat de kwetsbaarheid met kenmerk CVE-2026-20963 gericht en actief wordt misbruikt.

## Feiten

Microsoft heeft kwetsbaarheden verholpen in diverse Office-producten.

## Duiding

Een kwaadwillende kan de kwetsbaarheden misbruiken om 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 geauthenticeerd zijn op het kwetsbare systeem, of het slachtoffer misleiden een malafide bestand te openen of link te volgen.

Van de kwetsbaarheid met kenmerk CVE-2026-20963 wordt gemeld dat deze actief en gericht is misbruikt. De kwetsbaarheid stelt een kwaadwillende in staat om willekeurige code uit te voeren op een kwetsbaar Sharepoint systeem. Met name publiek toegankelijke installaties lopen verhoogd risico op misbruik. Buiten meldingen van actief misbruik is (nog) geen publieke Proof-of-Concept-code of exploit bekend. Door de media-aandacht echter, verwacht het NCSC dat deze wellicht op korte termijn beschikbaar komt, waardoor het risico op grootschalig misbruik zal toenemen.

### Microsoft Office Word:

CVE-ID	CVSS	Impact
CVE-2026-20944	7.80	Uitvoeren van willekeurige code
CVE-2026-20948	7.80	Uitvoeren van willekeurige code

### Microsoft Office SharePoint:

CVE-ID	CVSS	Impact
CVE-2026-20947	8.80	Uitvoeren van willekeurige code
CVE-2026-20951	7.80	Uitvoeren van willekeurige code
CVE-2026-20959	4.60	Voordoen als andere gebruiker
CVE-2026-20963	8.80	Uitvoeren van willekeurige code
CVE-2026-20958	5.40	Toegang tot gevoelige gegevens

|-----|-----|-----|

Microsoft Office:

CVE-ID	CVSS	Impact
CVE-2026-20943	7.00	Uitvoeren van willekeurige code
CVE-2026-20953	8.40	Uitvoeren van willekeurige code
CVE-2026-20952	8.40	Uitvoeren van willekeurige code

Microsoft Office Excel:

CVE-ID	CVSS	Impact
CVE-2026-20946	7.80	Uitvoeren van willekeurige code
CVE-2026-20955	7.80	Uitvoeren van willekeurige code
CVE-2026-20956	7.80	Uitvoeren van willekeurige code
CVE-2026-20949	7.80	Omzeilen van beveiligingsmaatregel
CVE-2026-20950	7.80	Uitvoeren van willekeurige code
CVE-2026-20957	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="#">CVE-2026-20943</a>	7.0 HIGH
> <a href="#">CVE-2026-20947</a>	8.8 HIGH
> <a href="#">CVE-2026-20951</a>	7.8 HIGH

> CVE-2026-20959	4.6 MEDIUM
> CVE-2026-20963	9.8 CRITICAL
> CVE-2026-20948	7.8 HIGH
> CVE-2026-20958	5.4 MEDIUM
> CVE-2026-20953	8.4 HIGH
> CVE-2026-20952	8.4 HIGH
> CVE-2026-20944	8.4 HIGH
> CVE-2026-20946	7.8 HIGH
> CVE-2026-20955	7.8 HIGH
> CVE-2026-20956	7.8 HIGH
> CVE-2026-20949	7.8 HIGH
> CVE-2026-20950	7.8 HIGH
> CVE-2026-20957	7.8 HIGH

## CWE's

CWE	Beschrijving
> CWE-20	Improper Input Validation
> 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-122	Heap-based Buffer Overflow
> CWE-125	Out-of-bounds Read
> CWE-191	Integer Underflow (Wrap or Wraparound)
> CWE-284	Improper Access Control

➤ CWE-416	Use After Free
➤ CWE-426	Untrusted Search Path
➤ CWE-502	Deserialization of Untrusted Data
➤ CWE-822	Untrusted Pointer Dereference
➤ CWE-918	Server-Side Request Forgery (SSRF)

## Getroffen producten

<b>Microsoft</b>
Microsoft 365 Apps for Enterprise
Microsoft 365 Apps for Enterprise for 32-bit Systems
Microsoft 365 Apps for Enterprise for 64-bit Systems
Microsoft Excel 2016
Microsoft Excel 2016 (32-bit edition)
Microsoft Excel 2016 (64-bit edition)
Microsoft Office 2016
Microsoft Office 2016 (32-bit edition)
Microsoft Office 2016 (64-bit edition)
Microsoft Office 2019
Microsoft Office 2019 for 32-bit editions

Microsoft Office 2019 for 64-bit editions
Microsoft Office Deployment Tool
Microsoft Office LTSC 2021
Microsoft Office LTSC 2021 for 32-bit editions
Microsoft Office LTSC 2021 for 64-bit editions
Microsoft Office LTSC 2024
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 SharePoint Enterprise Server 2016
Microsoft SharePoint Server 2019
Microsoft SharePoint Server Subscription Edition
Microsoft Word 2016
Microsoft Word 2016 (32-bit edition)
Microsoft Word 2016 (64-bit edition)

Office Online  
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.