Nationaal Cyber Security Centrum
Ministerie van Justitie en Veiligheid

NCSC-2026-0237

Kwetsbaarheden verholpen in Microsoft Office

NCSC Security Advisory

PRIORITEIT: HOOG

Gepubliceerd op: 21-07-2026
Revisie: 1.0.2

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).

Ontvangers van TLP:WHITE mogen de informatie publiek verspreiden.

Uw reacties zijn welkom op info@ncsc.nl

Update Revisie 2

Microsoft heeft in een update bevestigd dat SharePoint kwetsbaarheid CVE-2026-58644 actief als zeroday is misbruikt. Het NCSC raadt aan kwetsbare SharePoint systemen zo snel mogelijk te updaten naar de nieuwste versie om misbruik te voorkomen. De kwetsbaarheid CVE-2026-58644 betreft een deserialization-kwetsbaarheid welke misbruik zou kunnen worden om op afstand code uit te voeren. Mogelijk is de kwetsbaarheid CVE-2026-58644 in combinatie met SharePoint-kwetsbaarheid CVE-2026-56164 door kwaadwillende te misbruiken om zonder authenticatie op afstand code uit te voeren. De kwetsbaarheid CVE-2026-56164 betreft een privilegeescalation-kwetsbaarheid, deze zou misbruikt kunnen worden om rechten binnen een netwerk te verhogen.

Feiten

Microsoft heeft kwetsbaarheden verholpen in diverse Office producten, zoals Word, Excel, Powerpoint en SharePoint.

Duiding

Een kwaadwillende kan de kwetsbaarheden misbruiken om aanvallen uit te voeren die kunnen leiden tot categorieën schade, zoals benoemd in onderstaande tabel.

Voor succesvol misbruik moet de kwaadwillende het slachtoffer misleiden een malafide bestand te openen of link te volgen, met uitzondering van SharePoint. Voor succesvol misbruik van kwetsbaarheden in SharePoint is geen gebruikersinteractie nodig, anders dan het volgen van een malafide link.

Microsoft heeft in een update bevestigd dat SharePoint kwetsbaarheid CVE-2026-58644 actief als zeroday is misbruikt. Het NCSC raadt aan kwetsbare SharePoint systemen zo snel mogelijk te updaten naar de nieuwste versie om misbruik te voorkomen.

De kwetsbaarheid CVE-2026-58644 betreft een deserialization-kwetsbaarheid welke misbruik zou kunnen worden om op afstand code uit te voeren.

Mogelijk is de kwetsbaarheid CVE-2026-58644 in combinatie met SharePoint-kwetsbaarheid CVE-2026-56164 door kwaadwillende te misbruiken om zonder authenticatie op afstand code uit te voeren.

De kwetsbaarheid CVE-2026-56164 betreft een privilegeescalation-kwetsbaarheid, deze zou misbruikt kunnen worden om rechten binnen een netwerk te verhogen.

UPDATE: Volgens watchTowr is er een publieke exploit code voor SharePoint kwetsbaarheid CVE-2026-50522 gepubliceerd en wordt deze op on-premise versies van SharePoint nu ook actief misbruikt. Kwaadwillenden kunnen deze kwetsbaarheid misbruiken om zichzelf voor langere termijn toegang tot netwerken van kwetsbare systemen te verschaffen, door middel van het stelen van machine-keys.

Microsoft Office SharePoint:

CVE-ID	CVSS	Impact
CVE-2026-54108	6.50	Voordoen als andere gebruiker
CVE-2026-56164	5.30	Verkrijgen van verhoogde rechten
CVE-2026-50522	9.80	Uitvoeren van willekeurige code
CVE-2026-58644	9.80	Uitvoeren van willekeurige code
CVE-2026-55016	4.60	Voordoen als andere gebruiker
CVE-2026-55019	4.60	Voordoen als andere gebruiker
CVE-2026-55020	4.60	Voordoen als andere gebruiker
CVE-2026-55021	7.30	Voordoen als andere gebruiker
CVE-2026-55030	4.60	Voordoen als andere gebruiker
CVE-2026-55034	7.30	Voordoen als andere gebruiker
CVE-2026-55126	7.30	Voordoen als andere gebruiker
CVE-2026-55051	6.50	Toegang tot gevoelige gegevens
CVE-2026-55040	9.10	Omzeilen van beveiligingsmaatregel
CVE-2026-55052	8.80	Verkrijgen van verhoogde rechten
CVE-2026-55135	4.60	Voordoen als andere gebruiker
CVE-2026-56157	5.40	Voordoen als andere gebruiker
CVE-2026-58277	8.80	Verkrijgen van verhoogde rechten

Microsoft Office Word:

CVE-ID	CVSS	Impact
CVE-2026-55050	5.50	Toegang tot gevoelige gegevens
CVE-2026-55032	7.80	Uitvoeren van willekeurige code
CVE-2026-55033	7.80	Uitvoeren van willekeurige code
CVE-2026-55124	5.50	Uitvoeren van willekeurige code
CVE-2026-55127	7.80	Uitvoeren van willekeurige code
CVE-2026-55055	7.80	Uitvoeren van willekeurige code
CVE-2026-55038	7.80	Uitvoeren van willekeurige code
CVE-2026-55132	7.80	Uitvoeren van willekeurige code
CVE-2026-55134	7.80	Uitvoeren van willekeurige code
CVE-2026-55142	5.50	Toegang tot gevoelige gegevens
CVE-2026-55128	7.80	Uitvoeren van willekeurige code
CVE-2026-55130	7.80	Uitvoeren van willekeurige code

Microsoft Office PowerPoint:

CVE-ID	CVSS	Impact
CVE-2026-55043	7.80	Uitvoeren van willekeurige code
CVE-2026-55123	7.80	Uitvoeren van willekeurige code
CVE-2026-55120	7.80	Uitvoeren van willekeurige code

Microsoft Office:

CVE-ID	CVSS	Impact
CVE-2026-56193	7.10	Toegang tot gevoelige gegevens
CVE-2026-47290	7.80	Uitvoeren van willekeurige code
CVE-2026-50301	7.80	Uitvoeren van willekeurige code
CVE-2026-50314	7.80	Uitvoeren van willekeurige code
CVE-2026-50467	7.80	Uitvoeren van willekeurige code
CVE-2026-55017	7.80	Uitvoeren van willekeurige code
CVE-2026-55018	7.80	Uitvoeren van willekeurige code
CVE-2026-55022	7.80	Uitvoeren van willekeurige code
CVE-2026-55023	5.50	Toegang tot gevoelige gegevens
CVE-2026-55125	7.80	Uitvoeren van willekeurige code
CVE-2026-55026	6.20	Toegang tot gevoelige gegevens
CVE-2026-55027	5.50	Toegang tot gevoelige gegevens
CVE-2026-55028	5.50	Toegang tot gevoelige gegevens
CVE-2026-55047	5.50	Toegang tot gevoelige gegevens
CVE-2026-55045	8.40	Uitvoeren van willekeurige code
CVE-2026-55049	7.80	Uitvoeren van willekeurige code
CVE-2026-55129	7.80	Uitvoeren van willekeurige code
CVE-2026-55035	5.50	Toegang tot gevoelige gegevens
CVE-2026-55057	5.50	Toegang tot gevoelige gegevens
CVE-2026-55056	7.80	Uitvoeren van willekeurige code
CVE-2026-55140	7.80	Uitvoeren van willekeurige code
CVE-2026-55042	5.50	Toegang tot gevoelige gegevens
CVE-2026-55139	5.50	Toegang tot gevoelige gegevens
CVE-2026-50665	7.80	Toegang tot gevoelige gegevens
CVE-2026-56192	5.50	Toegang tot gevoelige gegevens
CVE-2026-56195	5.50	Toegang tot gevoelige gegevens

Microsoft Office OneNote:

CVE-ID	CVSS	Impact
CVE-2026-55133	7.80	Uitvoeren van willekeurige code

Microsoft Office Excel:

CVE-ID	CVSS	Impact
CVE-2026-50675	7.80	Uitvoeren van willekeurige code
CVE-2026-50678	6.60	Toegang tot gevoelige gegevens
CVE-2026-54988	6.10	Toegang tot gevoelige gegevens
CVE-2026-55899	7.80	Uitvoeren van willekeurige code
CVE-2026-55948	7.80	Uitvoeren van willekeurige code
CVE-2026-58618	7.80	Uitvoeren van willekeurige code
CVE-2026-47642	7.80	Uitvoeren van willekeurige code
CVE-2026-48580	5.50	Toegang tot gevoelige gegevens
CVE-2026-55024	7.80	Uitvoeren van willekeurige code
CVE-2026-50408	5.50	Toegang tot gevoelige gegevens
CVE-2026-55046	5.50	Toegang tot gevoelige gegevens
CVE-2026-55025	7.80	Uitvoeren van willekeurige code
CVE-2026-55031	7.80	Uitvoeren van willekeurige code
CVE-2026-55048	7.80	Uitvoeren van willekeurige code
CVE-2026-55029	7.80	Uitvoeren van willekeurige code
CVE-2026-55039	7.80	Uitvoeren van willekeurige code
CVE-2026-55041	7.80	Uitvoeren van willekeurige code
CVE-2026-55138	5.50	Toegang tot gevoelige gegevens
CVE-2026-55136	7.80	Uitvoeren van willekeurige code
CVE-2026-55141	7.80	Uitvoeren van willekeurige code
CVE-2026-55036	7.80	Uitvoeren van willekeurige code
CVE-2026-55044	7.80	Uitvoeren van willekeurige code
CVE-2026-55054	6.50	Toegang tot gevoelige gegevens
CVE-2026-55037	7.80	Uitvoeren van willekeurige code
CVE-2026-55058	7.80	Uitvoeren van willekeurige code
CVE-2026-55137	7.80	Uitvoeren van willekeurige code
CVE-2026-55053	7.80	Uitvoeren van willekeurige code
CVE-2026-55122	7.10	Toegang tot gevoelige gegevens
CVE-2026-55131	7.80	Uitvoeren van willekeurige code
CVE-2026-54131	7.80	Uitvoeren van willekeurige code

```
| CVE-2026-55898 | 6.10 | Toegang tot gevoelige gegevens      |
| CVE-2026-55947 | 7.80 | Uitvoeren van willekeurige code     |
| CVE-2026-55949 | 7.80 | Uitvoeren van willekeurige code     |
| CVE-2026-56156 | 7.80 | Uitvoeren van willekeurige code     |
|----------------|------|-------------------------------------|
```

Windows GDI:

```
|----------------|------|-------------------------------------|
| CVE-ID         | CVSS | Impact                              |
|----------------|------|-------------------------------------|
| CVE-2026-50387 | 7.80 | Verkrijgen van verhoogde rechten    |
|----------------|------|-------------------------------------|
```

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

Referenties

- https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2026-56164
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-58644
- https://portal.msrc.microsoft.com/en-us/security-guidance
- https://x.com/watchtowrcyber/status/2079512810766106905

Kwetsbaarheden

CVE	CVSS Score
CVE-2026-54108	6.5 MEDIUM
CVE-2026-56164	5.3 MEDIUM
CVE-2026-50522	9.8 CRITICAL
CVE-2026-58644	9.8 CRITICAL
CVE-2026-55016	4.6 MEDIUM

CVE-2026-55019	4.6 MEDIUM
CVE-2026-55020	4.6 MEDIUM
CVE-2026-55021	7.3 HIGH
CVE-2026-55023	5.5 MEDIUM
CVE-2026-55030	4.6 MEDIUM
CVE-2026-55125	7.8 HIGH
CVE-2026-55026	6.2 MEDIUM
CVE-2026-55034	7.3 HIGH
CVE-2026-55027	5.5 MEDIUM
CVE-2026-55028	5.5 MEDIUM
CVE-2026-55047	5.5 MEDIUM
CVE-2026-55045	8.4 HIGH
CVE-2026-55050	5.5 MEDIUM
CVE-2026-55032	7.8 HIGH
CVE-2026-55033	7.8 HIGH
CVE-2026-55124	5.5 MEDIUM
CVE-2026-55127	7.8 HIGH
CVE-2026-55035	5.5 MEDIUM
CVE-2026-55055	7.8 HIGH
CVE-2026-55038	7.8 HIGH
CVE-2026-55132	7.8 HIGH
CVE-2026-55126	7.3 HIGH
CVE-2026-55051	6.5 MEDIUM

CVE-2026-55134	7.8 HIGH
CVE-2026-55040	9.1 CRITICAL
CVE-2026-55142	5.5 MEDIUM
CVE-2026-55128	7.8 HIGH
CVE-2026-55130	7.8 HIGH
CVE-2026-55052	8.8 HIGH
CVE-2026-55135	4.6 MEDIUM
CVE-2026-56157	5.4 MEDIUM
CVE-2026-56192	5.5 MEDIUM
CVE-2026-58277	8.8 HIGH
CVE-2026-50675	7.8 HIGH
CVE-2026-50678	6.6 MEDIUM
CVE-2026-54988	6.1 MEDIUM
CVE-2026-55899	7.8 HIGH
CVE-2026-55948	7.8 HIGH
CVE-2026-58618	7.8 HIGH
CVE-2026-47642	7.8 HIGH
CVE-2026-48580	5.5 MEDIUM
CVE-2026-55024	7.8 HIGH
CVE-2026-50408	5.5 MEDIUM
CVE-2026-55046	5.5 MEDIUM
CVE-2026-55025	7.8 HIGH
CVE-2026-55031	7.8 HIGH

CVE-2026-55048	7.8 HIGH
CVE-2026-55029	7.8 HIGH
CVE-2026-55039	7.8 HIGH
CVE-2026-55041	7.8 HIGH
CVE-2026-55138	5.5 MEDIUM
CVE-2026-55136	7.8 HIGH
CVE-2026-55141	7.8 HIGH
CVE-2026-55036	7.8 HIGH
CVE-2026-55044	7.8 HIGH
CVE-2026-55054	6.5 MEDIUM
CVE-2026-55037	7.8 HIGH
CVE-2026-55058	7.8 HIGH
CVE-2026-55137	7.8 HIGH
CVE-2026-55053	7.8 HIGH
CVE-2026-55122	7.1 HIGH
CVE-2026-55131	7.8 HIGH
CVE-2026-54131	7.8 HIGH
CVE-2026-55898	6.1 MEDIUM
CVE-2026-55947	7.8 HIGH
CVE-2026-55949	7.8 HIGH
CVE-2026-56193	7.1 HIGH
CVE-2026-47290	7.8 HIGH
CVE-2026-50301	7.8 HIGH

CVE-2026-50314	7.8 HIGH
CVE-2026-50467	7.8 HIGH
CVE-2026-55017	7.8 HIGH
CVE-2026-55018	7.8 HIGH
CVE-2026-55022	7.8 HIGH
CVE-2026-55129	7.8 HIGH
CVE-2026-55057	5.5 MEDIUM
CVE-2026-55056	7.8 HIGH
CVE-2026-55140	7.8 HIGH
CVE-2026-55042	5.5 MEDIUM
CVE-2026-55139	5.5 MEDIUM
CVE-2026-55043	7.8 HIGH
CVE-2026-55123	7.8 HIGH
CVE-2026-55120	7.8 HIGH
CVE-2026-50665	7.8 HIGH
CVE-2026-56195	5.5 MEDIUM
CVE-2026-55133	7.8 HIGH
CVE-2026-56156	7.8 HIGH
CVE-2026-50387	7.8 HIGH
CVE-2026-55049	7.8 HIGH

CWE's

CWE	Beschrijving
CWE-20	Improper Input Validation

Getroffen producten

Microsoft
Microsoft 365 Apps for Enterprise for 32-bit Systems
Microsoft 365 Apps for Enterprise for 64-bit Systems
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 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 Office for Android
Microsoft PowerPoint 2016 (32-bit edition)
Microsoft PowerPoint 2016 (64-bit edition)
Microsoft SharePoint Enterprise Server 2016
Microsoft SharePoint Server 2019
Microsoft SharePoint Server Subscription Edition
Microsoft Word 2016 (32-bit edition)
Microsoft Word 2016 (64-bit edition)
Office Online Server

Disclaimer