Nationaal Cyber Security Centrum
Ministerie van Justitie en Veiligheid

Advisory NCSC-2026-0474

PRIORITEIT: NORMAAL

Kwetsbaarheden verholpen in Microsoft Office

Publicatiedatum: 10-11-2026

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 de-len. Dit staat beschreven in de standaard First (www.first.org/tlp).

Ontvangers van TLP:WHITE mogen de informatie publiek verspreiden.

Reacties zijn welkom op info@ncsc.nl.

Feiten

Microsoft heeft kwetsbaarheden verholpen in diverse Office producten.

Duiding

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

Microsoft heeft voor Office meerdere kwetsbaarheden verholpen. De 2 ernstigste kwetsbaarheden bevinden zich in Sharepoint en hebben een CVSS score van 9.0 en 9.9 toegewezen gekregen. Voor succesvol misbruik van een aantal kwetsbaarheden moet de kwaadwillende het slachtoffer misleiden om een malafide bestand te openen of een malafide link te volgen.

De kwetsbaarheid met kenmerk CVE-2026-109454 betreft cross-site scripting (XSS) in SharePoint. Een geautoriseerde kwaadwillende kan deze kwetsbaarheid via het netwerk misbruiken om spoofing uit te voeren. Voor de kwetsbaarheid met kenmerk CVE-2026-120002 geldt dat een geautoriseerde kwaadwillende door onvoldoende autorisatiecontroles in Microsoft Office SharePoint via het netwerk verhoogde rechten kan verkrijgen.

De overige kwetsbaarheden variëren in ernst van middelmatig tot hoog. Een samenvatting is in deze advisory opgenomen, maar het voert te ver om elke kwetsbaarheid in detail weer te geven. Raapleeg het MSRC-portaal voor aanvullende informatie.

Microsoft Teams:

CVE-ID	CVSS	Impact
CVE-2026-116926	7.50	Voordoen als andere gebruiker

Microsoft Office PowerPoint:

CVE-ID	CVSS	Impact
CVE-2026-109487	7.50	Uitvoeren van willekeurige code
CVE-2026-112734	8.80	Uitvoeren van willekeurige code
CVE-2026-112737	8.80	Uitvoeren van willekeurige code
CVE-2026-112738	6.50	Toegang tot gevoelige gegevens
CVE-2026-116922	6.50	Toegang tot gevoelige gegevens
CVE-2026-120001	8.80	Uitvoeren van willekeurige code
CVE-2026-120005	8.80	Uitvoeren van willekeurige code
CVE-2026-120787	7.50	Uitvoeren van willekeurige code

Microsoft Office Excel:

CVE-ID	CVSS	Impact
CVE-2026-111292	6.50	Toegang tot gevoelige gegevens

CVE-2026-116927	8.80	Uitvoeren van willekeurige code
CVE-2026-118292	8.80	Uitvoeren van willekeurige code
CVE-2026-118293	8.80	Uitvoeren van willekeurige code
CVE-2026-118294	8.80	Uitvoeren van willekeurige code
CVE-2026-118295	8.80	Uitvoeren van willekeurige code
CVE-2026-118296	8.80	Uitvoeren van willekeurige code
CVE-2026-118297	8.80	Uitvoeren van willekeurige code
CVE-2026-118298	8.80	Uitvoeren van willekeurige code
CVE-2026-118299	8.80	Uitvoeren van willekeurige code
CVE-2026-118300	6.50	Toegang tot gevoelige gegevens
CVE-2026-118301	7.50	Uitvoeren van willekeurige code
CVE-2026-118302	8.80	Uitvoeren van willekeurige code
CVE-2026-118700	8.80	Uitvoeren van willekeurige code
CVE-2026-118701	8.80	Uitvoeren van willekeurige code
CVE-2026-118702	8.80	Uitvoeren van willekeurige code
CVE-2026-118703	8.80	Uitvoeren van willekeurige code
CVE-2026-118704	8.80	Uitvoeren van willekeurige code
CVE-2026-118705	8.80	Uitvoeren van willekeurige code
CVE-2026-118706	8.80	Uitvoeren van willekeurige code
CVE-2026-118707	8.80	Uitvoeren van willekeurige code
CVE-2026-118708	8.80	Uitvoeren van willekeurige code
CVE-2026-118709	8.80	Uitvoeren van willekeurige code
CVE-2026-118710	8.80	Uitvoeren van willekeurige code
CVE-2026-118711	8.80	Uitvoeren van willekeurige code
CVE-2026-118712	8.80	Uitvoeren van willekeurige code
CVE-2026-118713	8.80	Uitvoeren van willekeurige code
CVE-2026-118714	8.80	Uitvoeren van willekeurige code
CVE-2026-118715	8.80	Verkrijgen van verhoogde rechten
CVE-2026-118716	8.80	Uitvoeren van willekeurige code
CVE-2026-118717	8.80	Uitvoeren van willekeurige code
CVE-2026-118718	8.80	Uitvoeren van willekeurige code
CVE-2026-118719	8.80	Uitvoeren van willekeurige code
CVE-2026-118720	8.80	Uitvoeren van willekeurige code
CVE-2026-118721	8.80	Uitvoeren van willekeurige code
CVE-2026-118722	8.80	Uitvoeren van willekeurige code
CVE-2026-118723	7.80	Uitvoeren van willekeurige code
CVE-2026-118724	8.80	Uitvoeren van willekeurige code
CVE-2026-118725	8.80	Verkrijgen van verhoogde rechten
CVE-2026-118726	8.80	Uitvoeren van willekeurige code
CVE-2026-118727	6.50	Toegang tot gevoelige gegevens
CVE-2026-118728	6.50	Toegang tot gevoelige gegevens
CVE-2026-118729	8.80	Uitvoeren van willekeurige code
CVE-2026-118730	8.80	Uitvoeren van willekeurige code
CVE-2026-118731	8.80	Uitvoeren van willekeurige code
CVE-2026-118732	8.80	Uitvoeren van willekeurige code
CVE-2026-119986	8.80	Uitvoeren van willekeurige code
CVE-2026-119999	6.50	Toegang tot gevoelige gegevens
CVE-2026-120785	8.80	Uitvoeren van willekeurige code
CVE-2026-120786	8.80	Uitvoeren van willekeurige code
CVE-2026-120788	8.80	Uitvoeren van willekeurige code
CVE-2026-120789	8.80	Uitvoeren van willekeurige code
CVE-2026-120790	8.80	Uitvoeren van willekeurige code
CVE-2026-120791	8.80	Uitvoeren van willekeurige code
CVE-2026-123385	8.80	Uitvoeren van willekeurige code
CVE-2026-123395	5.90	Toegang tot gevoelige gegevens

CVE-2026-124170	7.50	Uitvoeren van willekeurige code
CVE-2026-124172	7.50	Uitvoeren van willekeurige code
CVE-2026-124174	8.80	Uitvoeren van willekeurige code
CVE-2026-124176	8.80	Uitvoeren van willekeurige code
CVE-2026-124178	6.50	Toegang tot gevoelige gegevens
CVE-2026-124179	6.50	Toegang tot gevoelige gegevens
CVE-2026-124183	6.50	Toegang tot gevoelige gegevens
CVE-2026-124187	8.80	Uitvoeren van willekeurige code

Microsoft Office Outlook:

CVE-ID	CVSS	Impact
CVE-2026-110043	8.80	Uitvoeren van willekeurige code
CVE-2026-110068	8.80	Uitvoeren van willekeurige code
CVE-2026-111309	8.80	Uitvoeren van willekeurige code
CVE-2026-119993	6.50	Toegang tot gevoelige gegevens
CVE-2026-119995	7.50	Uitvoeren van willekeurige code
CVE-2026-119996	7.50	Uitvoeren van willekeurige code
CVE-2026-119997	7.80	Uitvoeren van willekeurige code
CVE-2026-123375	8.80	Uitvoeren van willekeurige code
CVE-2026-123376	8.80	Uitvoeren van willekeurige code
CVE-2026-123377	8.80	Uitvoeren van willekeurige code
CVE-2026-123378	7.50	Uitvoeren van willekeurige code
CVE-2026-123379	7.50	Uitvoeren van willekeurige code
CVE-2026-123380	8.80	Uitvoeren van willekeurige code
CVE-2026-123381	8.80	Uitvoeren van willekeurige code
CVE-2026-123382	8.80	Uitvoeren van willekeurige code
CVE-2026-123383	8.80	Uitvoeren van willekeurige code
CVE-2026-123384	8.80	Uitvoeren van willekeurige code
CVE-2026-124194	6.50	Voordoen als andere gebruiker

Microsoft Office Word:

CVE-ID	CVSS	Impact
CVE-2026-109491	7.50	Uitvoeren van willekeurige code
CVE-2026-109500	7.50	Uitvoeren van willekeurige code
CVE-2026-109501	8.80	Uitvoeren van willekeurige code
CVE-2026-109503	8.80	Uitvoeren van willekeurige code
CVE-2026-109505	8.80	Uitvoeren van willekeurige code
CVE-2026-110046	6.50	Toegang tot gevoelige gegevens
CVE-2026-110047	8.80	Uitvoeren van willekeurige code
CVE-2026-110048	8.80	Uitvoeren van willekeurige code
CVE-2026-110049	7.80	Uitvoeren van willekeurige code
CVE-2026-110050	8.80	Uitvoeren van willekeurige code
CVE-2026-110051	6.50	Toegang tot gevoelige gegevens
CVE-2026-110052	7.50	Uitvoeren van willekeurige code
CVE-2026-110053	7.50	Uitvoeren van willekeurige code
CVE-2026-110054	8.80	Uitvoeren van willekeurige code
CVE-2026-110055	8.80	Uitvoeren van willekeurige code
CVE-2026-110056	7.80	Uitvoeren van willekeurige code
CVE-2026-110061	8.80	Uitvoeren van willekeurige code

CVE-2026-110062	8.80	Uitvoeren van willekeurige code
CVE-2026-110064	8.80	Uitvoeren van willekeurige code
CVE-2026-110066	6.50	Toegang tot gevoelige gegevens
CVE-2026-110067	8.80	Uitvoeren van willekeurige code
CVE-2026-111285	8.80	Uitvoeren van willekeurige code
CVE-2026-111287	7.50	Uitvoeren van willekeurige code
CVE-2026-111288	6.50	Toegang tot gevoelige gegevens
CVE-2026-111290	8.80	Uitvoeren van willekeurige code
CVE-2026-111294	8.80	Uitvoeren van willekeurige code
CVE-2026-111295	8.80	Uitvoeren van willekeurige code
CVE-2026-111298	8.80	Uitvoeren van willekeurige code
CVE-2026-111299	8.80	Uitvoeren van willekeurige code
CVE-2026-111302	7.80	Uitvoeren van willekeurige code
CVE-2026-111304	8.80	Uitvoeren van willekeurige code
CVE-2026-111306	8.80	Uitvoeren van willekeurige code
CVE-2026-111307	8.80	Uitvoeren van willekeurige code
CVE-2026-111308	8.80	Uitvoeren van willekeurige code
CVE-2026-111310	8.80	Uitvoeren van willekeurige code
CVE-2026-112714	8.80	Uitvoeren van willekeurige code
CVE-2026-112715	8.80	Uitvoeren van willekeurige code
CVE-2026-112716	8.80	Uitvoeren van willekeurige code
CVE-2026-112717	8.80	Uitvoeren van willekeurige code
CVE-2026-112718	8.80	Uitvoeren van willekeurige code
CVE-2026-112719	8.80	Uitvoeren van willekeurige code
CVE-2026-112720	5.50	Toegang tot gevoelige gegevens
CVE-2026-112721	8.80	Uitvoeren van willekeurige code
CVE-2026-112722	8.80	Uitvoeren van willekeurige code
CVE-2026-112723	8.80	Uitvoeren van willekeurige code
CVE-2026-112724	8.80	Uitvoeren van willekeurige code
CVE-2026-112726	8.80	Uitvoeren van willekeurige code
CVE-2026-112728	8.80	Uitvoeren van willekeurige code
CVE-2026-112729	8.80	Uitvoeren van willekeurige code
CVE-2026-112730	8.80	Uitvoeren van willekeurige code
CVE-2026-112733	8.80	Uitvoeren van willekeurige code
CVE-2026-112735	8.80	Uitvoeren van willekeurige code
CVE-2026-112739	8.80	Uitvoeren van willekeurige code
CVE-2026-112741	8.80	Uitvoeren van willekeurige code
CVE-2026-113759	7.80	Uitvoeren van willekeurige code
CVE-2026-116718	7.50	Uitvoeren van willekeurige code
CVE-2026-116719	8.80	Uitvoeren van willekeurige code
CVE-2026-116720	8.80	Uitvoeren van willekeurige code
CVE-2026-116721	6.50	Toegang tot gevoelige gegevens
CVE-2026-116722	8.80	Uitvoeren van willekeurige code
CVE-2026-116923	8.80	Uitvoeren van willekeurige code
CVE-2026-116925	8.80	Uitvoeren van willekeurige code
CVE-2026-123394	8.80	Uitvoeren van willekeurige code
CVE-2026-124185	7.50	Uitvoeren van willekeurige code
CVE-2026-62804	7.80	Uitvoeren van willekeurige code

Microsoft Office Visio:

CVE-ID	CVSS	Impact
CVE-2026-109494	8.80	Uitvoeren van willekeurige code

| CVE-2026-109496 | 8.80 | Uitvoeren van willekeurige code |

Microsoft Teams for Android:

CVE-ID	CVSS	Impact
CVE-2026-122979	8.10	Voordoen als andere gebruiker
CVE-2026-69901	7.50	Voordoen als andere gebruiker

Microsoft Office OneNote:

CVE-ID	CVSS	Impact
CVE-2026-116924	8.80	Uitvoeren van willekeurige code
CVE-2026-119994	8.80	Uitvoeren van willekeurige code
CVE-2026-124181	7.50	Uitvoeren van willekeurige code

Microsoft Office:

CVE-ID	CVSS	Impact
CVE-2026-111286	7.50	Uitvoeren van willekeurige code
CVE-2026-111289	8.80	Uitvoeren van willekeurige code
CVE-2026-111291	6.50	Toegang tot gevoelige gegevens
CVE-2026-111293	6.50	Toegang tot gevoelige gegevens
CVE-2026-112731	6.50	Toegang tot gevoelige gegevens
CVE-2026-116717	8.80	Uitvoeren van willekeurige code
CVE-2026-119998	6.50	Omzeilen van beveiligingsmaatregel
CVE-2026-120003	8.80	Uitvoeren van willekeurige code
CVE-2026-122198	8.80	Uitvoeren van willekeurige code

Microsoft Office SharePoint:

CVE-ID	CVSS	Impact
CVE-2026-109454	9.00	Voordoen als andere gebruiker
CVE-2026-109455	6.50	Toegang tot gevoelige gegevens
CVE-2026-109464	8.80	Uitvoeren van willekeurige code
CVE-2026-109466	8.00	Verkrijgen van verhoogde rechten
CVE-2026-109472	8.80	Uitvoeren van willekeurige code
CVE-2026-109495	6.60	Verkrijgen van verhoogde rechten
CVE-2026-109497	7.30	Voordoen als andere gebruiker
CVE-2026-109499	8.80	Uitvoeren van willekeurige code
CVE-2026-109502	8.80	Verkrijgen van verhoogde rechten
CVE-2026-109504	7.30	Voordoen als andere gebruiker
CVE-2026-110044	8.80	Uitvoeren van willekeurige code
CVE-2026-110045	7.30	Voordoen als andere gebruiker
CVE-2026-110057	6.50	Toegang tot gevoelige gegevens
CVE-2026-110065	7.30	Voordoen als andere gebruiker
CVE-2026-111296	8.00	Verkrijgen van verhoogde rechten
CVE-2026-111297	8.00	Voordoen als andere gebruiker

CVE-2026-111300	7.30	Voordoen als andere gebruiker
CVE-2026-111303	7.30	Voordoen als andere gebruiker
CVE-2026-112736	5.30	Voordoen als andere gebruiker
CVE-2026-120000	7.50	Uitvoeren van willekeurige code
CVE-2026-120002	9.90	Verkrijgen van verhoogde rechten
CVE-2026-80095	9.00	Verkrijgen van verhoogde rechten
CVE-2026-88176	8.80	Verkrijgen van verhoogde rechten

Microsoft Office Access:

CVE-ID	CVSS	Impact
CVE-2026-109493	8.80	Uitvoeren van willekeurige code
CVE-2026-109498	7.50	Uitvoeren van willekeurige code
CVE-2026-110058	8.80	Uitvoeren van willekeurige code
CVE-2026-110059	8.80	Uitvoeren van willekeurige code
CVE-2026-110060	8.80	Uitvoeren van willekeurige code
CVE-2026-111301	8.80	Uitvoeren van willekeurige code
CVE-2026-111305	8.80	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

Referenties

- https://portal.msrc.microsoft.com/en-us/security-guidance

Kwetsbaarheden

CVE	CVSS Score
CVE-2026-109454	9.0 CRITICAL
CVE-2026-120002	9.9 CRITICAL

CWE's

CWE	Beschrijving
CWE-79	Improper Neutralization of Input During Web Page Generation
CWE-121	Stack-based Buffer Overflow
CWE-122	Heap-based Buffer Overflow
CWE-125	Out-of-bounds Read
CWE-126	Buffer Over-read
CWE-193	Off-by-one Error
CWE-197	Numeric Truncation Error
CWE-415	Double Free
CWE-416	Use After Free
CWE-502	Deserialization of Untrusted Data
CWE-639	Authorization Bypass Through User-Controlled Key
CWE-681	Incorrect Conversion between Numeric Types
CWE-822	Untrusted Pointer Dereference
CWE-843	Access of Resource Using Incompatible Type
CWE-862	Missing Authorization
CWE-863	Incorrect Authorization
CWE-918	Server-Side Request Forgery

Getroffen producten

Microsoft
Microsoft 365 Apps for Enterprise for 32-bit Systems
Microsoft 365 Apps for Enterprise for 64-bit Systems
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 SharePoint Server Subscription Edition

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.