



NCSC-2024-0251

Kwetsbaarheden verholpen in Microsoft Office

NCSC Advisory

Prioriteit: Normaal

Gepubliceerd op: 11-06-2024

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

Feiten

Microsoft heeft kwetsbaarheden verholpen in diverse Office producten.

Duiding

Een kwaadwillende kan de kwetsbaarheden misbruiken om willekeurige code uit te voeren met rechten van het slachtoffer, en daarmee mogelijk toegang te krijgen tot gevoelige gegevens in de context van het slachtoffer.

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

Microsoft Office Word:

CVE-ID	CVSS	Impact
CVE-2024-30102	7.30	Uitvoeren van willekeurige code

Microsoft Office:

CVE-ID	CVSS	Impact
CVE-2024-30101	7.50	Uitvoeren van willekeurige code
CVE-2024-30104	7.80	Uitvoeren van willekeurige code

Microsoft Office SharePoint:

CVE-ID	CVSS	Impact
CVE-2024-30100	7.80	Uitvoeren van willekeurige code

Microsoft Office Outlook:

CVE-ID	CVSS	Impact
CVE-2024-30103	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>

Kwetsbaarheden

CVE	CVSS Score
> CVE-2024-30100	7.8 HIGH
> CVE-2024-30101	7.5 HIGH
> CVE-2024-30102	7.3 HIGH
> CVE-2024-30103	8.8 HIGH
> CVE-2024-30104	7.8 HIGH

CWE's

CWE	Beschrijving
> CWE-184	Incomplete List of Disallowed Inputs
> CWE-416	Use After Free
> CWE-426	Untrusted Search Path
> CWE-59	Improper Link Resolution Before File Access ('Link Following')

Getroffen producten

microsoft
365_apps_for_enterprise
microsoft_365_apps_for_enterprise

microsoft_office_2016
microsoft_office_2019
microsoft_office_ltsc_2021
microsoft_outlook_2016
microsoft_sharepoint_enterprise_server_2016
microsoft_sharepoint_server_2019
microsoft_sharepoint_server_subscription_edition
office
outlook
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.