



NCSC-2024-0365

Kwetsbaarheden verholpen in Microsoft Office

NCSC Advisory

Prioriteit: Normaal

Gepubliceerd op: 10-09-2024

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 een Denial-of-Service te veroorzaken, zich verhoogde rechten toe te kennen, toegang te krijgen tot gevoelige gegevens of code uit te voeren met mogelijk SYSTEM-rechten.

Voor succesvol misbruik van de kwetsbaarheden moet de kwaadwillende het slachtoffer misleiden een malafide bestand te openen of link te volgen naar een webserver onder controle van de kwaadwillende.

Van de kwetsbaarheid met kenmerk CVE-2024-38226 geeft Microsoft aan informatie te hebben dat deze beperkt en gericht is misbruikt. De kwetsbaarheid bevindt zich in Publisher en stelt een kwaadwillende in staat om beperkingen rond de uitvoer van macro's te omzeilen en zo macro-code uit te voeren in de context van het slachtoffer. Er is (nog) geen publieke Proof-of-Concept-code of exploit bekend.

Microsoft Office SharePoint:

CVE-ID	CVSS	Impact
CVE-2024-38018	8.80	Uitvoeren van willekeurige code
CVE-2024-43464	7.20	Uitvoeren van willekeurige code
CVE-2024-38227	7.20	Uitvoeren van willekeurige code
CVE-2024-38228	7.20	Uitvoeren van willekeurige code
CVE-2024-43466	6.50	Denial-of-Service

Microsoft Office Publisher:

CVE-ID	CVSS	Impact
CVE-2024-38226	7.30	Omzeilen van beveiligingsmaatregel

Microsoft Graphics Component:

CVE-ID	CVSS	Impact
CVE-2024-38250	7.80	Verkrijgen van verhoogde rechten

Microsoft Office Visio:

CVE-ID	CVSS	Impact
CVE-2024-43463	7.80	Uitvoeren van willekeurige code

Microsoft AutoUpdate (MAU):

CVE-ID	CVSS	Impact
CVE-2024-43492	7.80	Verkrijgen van verhoogde rechten

Microsoft Office Excel:

CVE-ID	CVSS	Impact
CVE-2024-43465	7.80	Verkrijgen van verhoogde rechten

Microsoft Outlook for iOS:

CVE-ID	CVSS	Impact
CVE-2024-43482	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-2024-38018	
> CVE-2024-43464	
> CVE-2024-38227	7.2 HIGH
> CVE-2024-38228	
> CVE-2024-43466	
> CVE-2024-38250	7.8 HIGH
> CVE-2024-43465	
> CVE-2024-43463	
> CVE-2024-38226	
> CVE-2024-43482	
> CVE-2024-43492	7.8 HIGH

CWE's

CWE	Beschrijving
> CWE-126	Buffer Over-read
> CWE-77	Improper Neutralization of Special Elements used in a Command ('Command Injection')
> CWE-693	Protection Mechanism Failure
> CWE-285	Improper Authorization
> CWE-284	Improper Access Control
> CWE-416	Use After Free
> CWE-502	Deserialization of Untrusted Data

Getroffen producten

microsoft
microsoft_365_apps_for_enterprise
microsoft_autoupdate_for_mac
microsoft_excel_2016
microsoft_office_2019
microsoft_office_for_android
microsoft_office_for_universal
microsoft_office_ltsc_2021
microsoft_office_ltsc_for_mac_2021
microsoft_office_online_server
microsoft_publisher_2016
microsoft_sharepoint_enterprise_server_2016
microsoft_sharepoint_server_2019
microsoft_sharepoint_server_subscription_edition
microsoft_visio_2016
outlook_for_ios

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.