Nationaal Cyber Security Centrum
Ministerie van Justitie en Veiligheid

NCSC-2024-0471

Kwetsbaarheden verholpen in Microsoft Office

NCSC Advisory
Prioriteit: Normaal
Gepubliceerd op: 10-12-2024

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 zich verhoogde rechten toe te kennen, willekeurige code uit te voeren in de context van het slachtoffer en mogelijk toegang te krijgen tot gevoelige informatie in de context van het slachtoffer. Voor succesvol misbruik moet de kwaadwillende het slachtoffer misleiden een malafide bestand te openen of link te volgen.

Naast de verholpen kwetsbaarheden heeft Microsoft ook een update uitgebracht om de Defense In-Depth van MS Project 2016 te verbeteren. Inzet van deze update vereist mogelijk een handmatige actie. Zie hiervoor het gepubliceerde artikel ADV240002

Microsoft Office SharePoint:

CVE-ID	CVSS	Impact
CVE-2024-49064	6.50	Toegang tot gevoelige gegevens
CVE-2024-49068	8.20	Verkrijgen van verhoogde rechten
CVE-2024-49070	7.40	Uitvoeren van willekeurige code
CVE-2024-49062	6.50	Toegang tot gevoelige gegevens

Microsoft Office Word:

CVE-ID	CVSS	Impact
CVE-2024-49065	5.50	Uitvoeren van willekeurige code

Microsoft Office Access:

CVE-ID	CVSS	Impact
CVE-2024-49142	7.80	Uitvoeren van willekeurige code

Microsoft Office:

CVE-ID	CVSS	Impact
CVE-2024-49059	7.00	Verkrijgen van verhoogde rechten
CVE-2024-43600	7.80	Verkrijgen van verhoogde rechten

Microsoft Office Excel:

CVE-ID	CVSS	Impact
CVE-2024-49069	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

Referenties

- https://www.microsoft.com/download/details.aspx?familyid=3fae2662-eabf-4fb7-93c9-08e94bccfdc0

Kwetsbaarheden

CVE	CVSS Score
CVE-2024-49059	7.0 HIGH
CVE-2024-49069	7.8 HIGH
CVE-2024-49142	7.8 HIGH
CVE-2024-49065	5.5 MEDIUM
CVE-2024-43600	7.8 HIGH
CVE-2024-49064	6.5 MEDIUM

CVE-2024-49068	8.2 HIGH
CVE-2024-49070	7.4 HIGH
CVE-2024-49062	6.5 MEDIUM

CWE's

CWE	Beschrijving
CWE-59	Improper Link Resolution Before File Access ('Link Following')
CWE-23	Relative Path Traversal
CWE-125	Out-of-bounds Read
CWE-284	Improper Access Control
CWE-416	Use After Free
CWE-502	Deserialization of Untrusted Data
CWE-611	Improper Restriction of XML External Entity Reference

Getroffen producten

microsoft
365_apps
access
excel
microsoft_365_apps_for_enterprise
microsoft_access_2016__32-bit_edition_
microsoft_access_2016__64-bit_edition_
microsoft_excel_2016
microsoft_office_2016

microsoft_office_2019
microsoft_office_ltsc_2021
microsoft_office_ltsc_2024
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
office
office_long_term_servicing_channel
sharepoint_server

Disclaimer