Nationaal Cyber Security Centrum
Ministerie van Justitie en Veiligheid

Advisory NCSC-2024-0337

Kwetsbaarheden verholpen in Microsoft Office

2024-08-13 Revisie 0

Toegestande verspreiding: 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.firs t.org/tlp). Ontvangers mogen de informatie delen met collega's van andere organisaties, informatiefora of personen werkzaam in netwerkbeveiliging, informatiebeveiliging of de VI-gemeenschap in de bredere zin. Het is niet de bedoeling dat u de informatie publiek maakt.

Uw reacties zijn welkom op info@ncsc.nl

Feiten

Microsoft heeft kwetsbaarheden verholpen in diverse Office producten.

Interpretaties

Een kwaadwillende kan de kwetsbaarheden misbruiken om zich voor te doen als andere gebruiker, willekeurige code uit te voeren met rechten van het slachtoffer en 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 of link te volgen.

``` Microsoft Teams: |----------|------|----------| | CVE-ID | CVSS | Impact | |----------|------|----------| | CVE-2024-38197 | 6.50 | Voordoen als andere gebruiker | |----------|------|----------|

Microsoft Office: |----------|------|----------| | CVE-ID | CVSS | Impact | |----------|------|----------| | CVE-2024-38084 | 7.80 | Verkrijgen van verhoogde rechten | | CVE-2024-38200 | 7.50 | Voordoen als andere gebruiker | |----------|------|----------|

Microsoft Office Outlook: |----------|------|----------| | CVE-ID | CVSS | Impact | |----------|------|----------| | CVE-2024-38173 | 6.70 | Uitvoeren van willekeurige code | |----------|------|----------|

Microsoft Office Visio: |----------|------|----------| | CVE-ID | CVSS | Impact | |----------|------|----------| | CVE-2024-38169 | 7.80 | Uitvoeren van willekeurige code | |----------|------|----------|

Microsoft Office Project: |----------|------|----------| | CVE-ID | CVSS | Impact | |----------|------|----------| | CVE-2024-38189 | 8.80 | Uitvoeren van willekeurige code | |----------|------|----------|

Microsoft Office PowerPoint: |----------|------|----------| | CVE-ID | CVSS | Impact | |----------|------|----------| | CVE-2024-38171 | 7.80 | Uitvoeren van willekeurige code | |----------|------|----------|

Microsoft Copilot Studio: |----------|------|----------| | CVE-ID | CVSS | Impact | |----------|------|----------| | CVE-2024-38206 | 8.50 | Toegang tot gevoelige gegevens | |----------|------|----------|

Microsoft Office Excel: |----------|------|----------| | CVE-ID | CVSS | Impact | |----------|------|----------| | CVE-2024-38172 | 7.80 | Uitvoeren van willekeurige code | |
```

CVE-2024-38170 | 7.10 | 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