Nationaal Cyber Security Centrum
Ministerie van Justitie en Veiligheid

Advisory NCSC-2024-0365

Kwetsbaarheden verholpen in Microsoft Office

2024-09-10 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 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