Nationaal Cyber Security Centrum
Ministerie van Justitie en Veiligheid

Advisory NCSC-2024-0397

Kwetsbaarheden verholpen in Microsoft System Center

2024-10-08 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 System Center.

Interpretaties

Een kwaadwillende kan de kwetsbaarheden misbruiken om zich voor te doen als andere gebruiker, of om willekeurige code uit te voeren met rechten van een administrator.

Om succesvol code-uitvoer te bereiken moet de kwaadwillende LAN-toegang hebben tot het systeem waarop Configuration Manager is geïmplementeerd en draait. De kwaadwillende moet dan speciaal geprepareerd netwerkverkeer naar dit systeem versturen.

``` Microsoft Configuration Manager:
|----------|------|----------| | CVE-ID | CVSS | Impact |
|----------|------|----------| | CVE-2024-43468 | 9.80 | Uitvoeren van willekeurige code |
|----------|------|----------|

Microsoft Defender for Endpoint:
|----------|------|----------| | CVE-ID | CVSS | Impact |
|----------|------|----------| | CVE-2024-43614 | 5.50 | Voordoen als andere gebruiker |
|----------|------|----------| ```

## 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
```