Nationaal Cyber Security Centrum
Ministerie van Justitie en Veiligheid

Advisory NCSC-2024-0367

Kwetsbaarheden verholpen in Microsoft Dynamics

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 Dynamics.

Interpretaties

Een kwaadwillende kan de kwetsbaarheden misbruiken om zich verhoogde rechten toe te kennen en zo mogelijk code uit te voeren binnen de applicatie, of om een Cross-Site-Scripting-aanval uit te voeren. Een dergelijke aanval kan leiden tot uitvoer van code in de browser van het slachtoffer, of toegang tot gevoelige gegevens in de context van de browser van het slachtoffer.

``` Dynamics Business Central:
|---------------|------|-----------------------------------| | CVE-ID | CVSS | Impact |
|---------------|------|-----------------------------------| | CVE-2024-38225 | 8.80 |
Verkrijgen van verhoogde rechten |
|---------------|------|-----------------------------------|

Microsoft Dynamics 365 (on-premises):
|---------------|------|-----------------------------------| | CVE-ID | CVSS | Impact |
|---------------|------|-----------------------------------| | CVE-2024-43476 | 7.60 |
Voordoen als andere gebruiker |
|---------------|------|-----------------------------------|

Power Automate: |---------------|------|-----------------------------------| | CVE-ID |
CVSS | Impact | |---------------|------|-----------------------------------| |
CVE-2024-43479 | 8.50 | 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
```