



## Advisory NCSC-2024-0249

# Kwetsbaarheden verholpen in Microsoft Azure

2024-06-11 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.first.org/tlp](http://www.first.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](mailto:info@ncsc.nl)

## Feiten

Microsoft heeft kwetsbaarheden verholpen in Azure producten.

## Interpretaties

Een kwaadwillende kan de kwetsbaarheden misbruiken om een Denial-of-Service te veroorzaken, of om zich verhoogde rechten toe te kennen en mogelijk handelingen uit te voeren met beheerdersrechten.

De ernstigste kwetsbaarheid heeft kenmerk CVE-2024-37325 toegewezen gekregen. Deze kwetsbaarheid bevindt zich in de Data Science Virtual Machines met versies kleiner dan 24.05.24 welke draaien op Linux/Ubuntu. Een ongeauthenticeerde kwaadwillende kan de gebruikersgegevens van deze VM's achterhalen en inloggen als het slachtoffer.

```
``` Azure Storage Library: |-----|----|-----| |
CVE-ID | CVSS | Impact | |-----|----|-----| |
CVE-2024-35252 | 7.50 | Denial-of-Service |
|-----|----|-----|
```

```
Azure Monitor: |-----|----|-----| | CVE-ID |
CVSS | Impact | |-----|----|-----| |
CVE-2024-35254 | 7.10 | Verkrijgen van verhoogde rechten |
|-----|----|-----|
```

```
Azure File Sync: |-----|----|-----| | CVE-ID |
CVSS | Impact | |-----|----|-----| |
CVE-2024-35253 | 4.40 | Verkrijgen van verhoogde rechten |
|-----|----|-----|
```

```
Azure Data Science Virtual Machines:
|-----|----|-----| | CVE-ID | CVSS | Impact |
|-----|----|-----| | CVE-2024-37325 | 9.80 |
Verkrijgen van verhoogde rechten |
|-----|----|-----|
```

```
Azure SDK: |-----|----|-----| | CVE-ID | CVSS |
Impact | |-----|----|-----| | CVE-2024-35255 |
5.50 | Verkrijgen van verhoogde rechten |
|-----|----|-----| ```
```

## 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>