Nationaal Cyber Security Centrum
Ministerie van Justitie en Veiligheid

NCSC-2024-0249

Kwetsbaarheden verholpen in Microsoft Azure

NCSC Advisory
Prioriteit: Normaal
Gepubliceerd op: 11-06-2024

TLP:WHITE

Toegestane verspreiding van 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).

Ontvangers van TLP:WHITE mogen de informatie publiek verspreiden.

Uw reacties zijn welkom op info@ncsc.nl

Feiten

Microsoft heeft kwetsbaarheden verholpen in Azure producten.

Duiding

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

Kwetsbaarheden

CVE	CVSS Score
CVE-2024-35252	7.5 HIGH
CVE-2024-35253	4.4 MEDIUM
CVE-2024-35254	7.1 HIGH
CVE-2024-35255	5.5 MEDIUM
CVE-2024-37325	8.1 HIGH

CWE's

CWE	Beschrijving
CWE-1104	Use of Unmaintained Third Party Components
CWE-200	Exposure of Sensitive Information to an Unauthorized Actor
CWE-362	Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')
CWE-59	Improper Link Resolution Before File Access ('Link Following')

Getroffen producten

microsoft
azure_data_science_virtual_machines
azure_file_sync
azure_identity_library_for_.net
azure_identity_library_for_c__
azure_identity_library_for_java
azure_identity_library_for_javascript
azure_identity_library_for_python
azure_identity_library
azure_monitor
azure_storage
microsoft_authentication_library

Disclaimer