



# 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](http://www.first.org/tlp)).

Ontvangers van TLP:WHITE mogen de informatie publiek verspreiden.

Uw reacties zijn welkom op [info@ncsc.nl](mailto: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
> <a href="#">CVE-2024-35252</a>	7.5 HIGH
> <a href="#">CVE-2024-35253</a>	4.4 MEDIUM
> <a href="#">CVE-2024-35254</a>	7.1 HIGH
> <a href="#">CVE-2024-35255</a>	5.5 MEDIUM
> <a href="#">CVE-2024-37325</a>	8.1 HIGH

## CWE's

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

## Getroffen producten

<b>microsoft</b>
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

The Netherlands Cyber Security Center (henceforth: NCSC-NL) maintains this page to enhance access to its information and security advisories. The use of this security advisory is subject to the following terms and conditions: NCSC-NL makes every reasonable effort to ensure that the content of this page is kept up to date, and that it is accurate and complete. Nevertheless, NCSC-NL cannot entirely rule out the possibility of errors, and therefore cannot give any warranty in respect of its completeness, accuracy or continuous keeping up-to-date. The information contained in this security advisory is intended solely for the purpose of providing general information to professional users. No rights can be derived from the information provided therein. NCSC-NL and the Kingdom of the Netherlands assume no legal liability or responsibility for any damage resulting from either the use or inability of use of this security advisory. This includes damage resulting from the inaccuracy of incompleteness of the information contained in the advisory. This security advisory is subject to Dutch law. All disputes related to or arising from the use of this advisory will be submitted to the competent court in The Hague. This choice of means also applies to the court in summary proceedings.