



# NCSC-2024-0285

## Kwetsbaarheden verholpen in Microsoft Azure

NCSC Advisory

Prioriteit: Normaal

Gepubliceerd op: 09-07-2024

**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 diverse Azure componenten.

## Duiding

De kwetsbaarheden stellen een kwaadwillende in staat om zich voor te doen als andere gebruiker, zich verhoogde rechten te te kennen en mogelijk willekeurige code uit te voeren.

Een deel van de kwetsbaarheden bevindt zich in ontwikkel-tooling en is niet zondermeer voor ongeautoriseerde gebruikers toegankelijk.

### Azure CycleCloud:

CVE-ID	CVSS	Impact
CVE-2024-38092	8.80	Verkrijgen van verhoogde rechten

### Azure Network Watcher:

CVE-ID	CVSS	Impact
CVE-2024-35261	7.80	Verkrijgen van verhoogde rechten

### Azure DevOps:

CVE-ID	CVSS	Impact
CVE-2024-35266	7.60	Voordoen als andere gebruiker
CVE-2024-35267	7.60	Voordoen als andere gebruiker

### Azure Kinect SDK:

CVE-ID	CVSS	Impact
CVE-2024-38086	6.40	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>

## Dreigingsinformatie

### Kwetsbaarheden

CVE	CVSS Score
<a href="#">&gt; CVE-2024-38086</a>	6.4 MEDIUM
<a href="#">&gt; CVE-2024-35261</a>	
<a href="#">&gt; CVE-2024-35266</a>	7.6 HIGH
<a href="#">&gt; CVE-2024-35267</a>	
<a href="#">&gt; CVE-2024-38092</a>	

### CWE's

CWE	Beschrijving
<a href="#">&gt; CWE-197</a>	Numeric Truncation Error
<a href="#">&gt; CWE-59</a>	Improper Link Resolution Before File Access ('Link Following')
<a href="#">&gt; CWE-693</a>	Protection Mechanism Failure
<a href="#">&gt; CWE-79</a>	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')

## Getroffen producten

<b>microsoft</b>
azure_cyclecloud_7.9.0
azure_cyclecloud_7.9.1
azure_cyclecloud_7.9.10
azure_cyclecloud_7.9.11
azure_cyclecloud_7.9.2
azure_cyclecloud_7.9.3
azure_cyclecloud_7.9.4
azure_cyclecloud_7.9.6
azure_cyclecloud_7.9.7
azure_cyclecloud_7.9.8
azure_cyclecloud_7.9.9
azure_cyclecloud_8.0.0
azure_cyclecloud_8.0.1
azure_cyclecloud_8.0.2
azure_cyclecloud_8.1.0
azure_cyclecloud_8.1.1
azure_cyclecloud_8.2.0
azure_cyclecloud_8.2.1
azure_cyclecloud_8.2.2
azure_cyclecloud_8.3.0
azure_cyclecloud_8.4.0
azure_cyclecloud_8.4.1
azure_cyclecloud_8.4.2

azure_cyclecloud_8.5.0
azure_cyclecloud_8.6.0
azure_devops_server_2022
azure_kinect_sdk
azure_network_watcher_vm_extension

## 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 or 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.