



# NCSC-2024-0366

## Kwetsbaarheden verholpen in Microsoft Azure

NCSC Advisory

Prioriteit: Normaal

Gepubliceerd op: 10-09-2024

**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

Een kwaadwillende kan de kwetsbaarheden misbruiken om zich verhoogde rechten toe te kennen, toegang te krijgen tot gevoelige gegevens en mogelijk opdrachten uit te voeren met rechten van de Administrator.

Misbruik is niet eenvoudig en vereist voorafgaande authenticatie en kennis van de inrichting van de Azure-omgeving.

### Azure Network Watcher:

CVE-ID	CVSS	Impact
CVE-2024-38188	7.10	Verkrijgen van verhoogde rechten
CVE-2024-43470	7.30	Toegang tot gevoelige gegevens

### Azure CycleCloud:

CVE-ID	CVSS	Impact
CVE-2024-43469	8.80	Uitvoeren van willekeurige code

### Azure Stack:

CVE-ID	CVSS	Impact
CVE-2024-38216	8.20	Verkrijgen van verhoogde rechten
CVE-2024-38220	9.00	Verkrijgen van verhoogde rechten

### Azure Web Apps:

CVE-ID	CVSS	Impact
CVE-2024-38194	8.40	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="#">&gt; CVE-2024-38216</a>	8.2 HIGH
<a href="#">&gt; CVE-2024-38220</a>	9.0 CRITICAL
<a href="#">&gt; CVE-2024-38188</a>	
<a href="#">&gt; CVE-2024-43470</a>	
<a href="#">&gt; CVE-2024-43469</a>	
<a href="#">&gt; CVE-2024-38194</a>	8.4 HIGH

## CWE's

CWE	Beschrijving
<a href="#">&gt; CWE-59</a>	Improper Link Resolution Before File Access ('Link Following')
<a href="#">&gt; CWE-284</a>	Improper Access Control
<a href="#">&gt; CWE-94</a>	Improper Control of Generation of Code ('Code Injection')
<a href="#">&gt; CWE-20</a>	Improper Input Validation

## Getroffen producten

<b>microsoft</b>
azure_cyclecloud
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_network_watcher_vm_extension
azure_stack_hub
azure_web_apps

## 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.