



NCSC-2024-0335

Kwetsbaarheden verholpen in Microsoft Azure componenten

NCSC Advisory

Prioriteit: Normaal

Gepubliceerd op: 13-08-2024

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 diverse Azure componenten.

Duiding

Een kwaadwillende kan de kwetsbaarheden misbruiken om zich verhoogde rechten toe te kennen of zich voor te doen als andere gebruiker. Voor succesvol misbruik heeft de kwaadwillende voorafgaande toegang nodig tot de kwetsbare omgeving, of moet de kwaadwillende het slachtoffer misleiden een malafide bestand te openen of link te volgen.

Azure Connected Machine Agent:

CVE-ID	CVSS	Impact
CVE-2024-38098	7.80	Verkrijgen van verhoogde rechten
CVE-2024-38162	7.80	Verkrijgen van verhoogde rechten

Azure Stack:

CVE-ID	CVSS	Impact
CVE-2024-38108	9.30	Voordoene als andere gebruiker
CVE-2024-38201	7.00	Verkrijgen van verhoogde rechten

Azure CycleCloud:

CVE-ID	CVSS	Impact
CVE-2024-38195	7.80	Uitvoeren van willekeurige code

Azure Health Bot:

CVE-ID	CVSS	Impact
CVE-2024-38109	9.10	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>

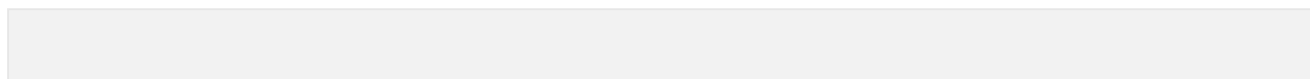
Kwetsbaarheden

CVE	CVSS Score
> CVE-2024-38108	9.3 CRITICAL
> CVE-2024-38201	7.0 HIGH
> CVE-2024-38098	7.8 HIGH
> CVE-2024-38162	7.8 HIGH
> CVE-2024-38195	7.8 HIGH
> CVE-2024-38109	9.1 CRITICAL

CWE's

CWE	Beschrijving
> CWE-20	Improper Input Validation
> CWE-284	Improper Access Control
> CWE-59	Improper Link Resolution Before File Access ('Link Following')
> CWE-79	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')
> CWE-918	Server-Side Request Forgery (SSRF)

Getroffen producten



microsoft
azure_connected_machine_agent
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_cyclecloud
azure_health_bot
azure_stack_hub

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.