Nationaal Cyber Security Centrum
Ministerie van Justitie en Veiligheid

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).

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, 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
CVE-2024-38216	8.2 HIGH
CVE-2024-38220	9.0 CRITICAL
CVE-2024-38188	
CVE-2024-43470	
CVE-2024-43469	
CVE-2024-38194	8.4 HIGH

CWE's

CWE	Beschrijving
CWE-59	Improper Link Resolution Before File Access ('Link Following')
CWE-284	Improper Access Control
CWE-94	Improper Control of Generation of Code ('Code Injection')
CWE-20	Improper Input Validation

Getroffen producten

microsoft
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