Nationaal Cyber Security Centrum
Ministerie van Justitie en Veiligheid

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).

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

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
CVE-2024-38086	6.4 MEDIUM
CVE-2024-35261	
CVE-2024-35266	7.6 HIGH
CVE-2024-35267	
CVE-2024-38092	

CWE's

CWE	Beschrijving
CWE-197	Numeric Truncation Error
CWE-59	Improper Link Resolution Before File Access ('Link Following')
CWE-693	Protection Mechanism Failure
CWE-79	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')

Getroffen producten

microsoft
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