Nationaal Cyber Security Centrum
Ministerie van Justitie en Veiligheid

Advisory NCSC-2024-0285

Kwetsbaarheden verholpen in Microsoft Azure

2024-07-09 Revisie 0

Toegestande verspreiding: 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.firs t.org/tlp). Ontvangers mogen de informatie delen met collega's van andere organisaties, informatiefora of personen werkzaam in netwerkbeveiliging, informatiebeveiliging of de VI-gemeenschap in de bredere zin. Het is niet de bedoeling dat u de informatie publiek maakt.

Uw reacties zijn welkom op info@ncsc.nl

Feiten

Microsoft heeft kwetsbaarheden verholpen in diverse Azure componenten.

Interpretaties

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