Nationaal Cyber Security Centrum
Ministerie van Justitie en Veiligheid

NCSC-2026-0347

Kwetsbaarheden verholpen in Microsoft Azure

NCSC Security Advisory
Prioriteit: Normaal
Gepubliceerd op: 08-09-2026

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 4 kwetsbaarheden verholpen in diverse Azure componenten.

Duiding

Een kwaadwillende kan de kwetsbaarheden misbruiken om aanvallen uit te voeren die kunnen leiden tot de categorieën schade, zoals genoemd in onderstaande tabel.

De kwetsbaarheid met kenmerk CVE-2026-69854 heeft een CVSS-score van 9,0. Een kwaadwillende die al over een geldige sessie beschikt, kan de kwetsbaarheid onder specifieke voorwaarden, zoals bepaalde protocolinstellingen of configuraties, misbruiken om zijn rechten binnen de applicatie te verhogen. Hierdoor kan de kwaadwillende toegang krijgen tot afgeschermde functionaliteiten of gegevens.

De kwetsbaarheid met kenmerk CVE-2026-62895 heeft een CVSS-score van 8,8. Een kwaadwillende kan een speciaal geprepareerde website hosten en een gebruiker ertoe verleiden deze te bezoeken. Vervolgens kan de kwaadwillende via verzoeken aan een kwetsbare lokaal draaiende service opdrachten uitvoeren met verhoogde rechten. Voor misbruik is geen authenticatie vereist, maar gebruikersinteractie is wel vereist. Succesvol misbruik kan leiden tot het verkrijgen van SYSTEM-rechten.

De kwetsbaarheid met kenmerk CVE-2026-77909 heeft een CVSS-score van 7,7. De kwetsbaarheid betreft onvoldoende beveiligde inloggegevens in Azure CycleCloud. Een geauthenticeerde kwaadwillende kan deze kwetsbaarheid via het netwerk misbruiken om informatie, waaronder inloggegevens, te verkrijgen.

```
Spring Cloud Azure:
|----------------|------|-------------------------------------|
| CVE-ID         | CVSS | Impact                              |
|----------------|------|-------------------------------------|
| CVE-2026-69854 | 9,00 | Verkrijgen van verhoogde rechten    |
|----------------|------|-------------------------------------|

Azure Arc:
|----------------|------|-------------------------------------|
| CVE-ID         | CVSS | Impact                              |
|----------------|------|-------------------------------------|
| CVE-2026-62895 | 8,80 | Verkrijgen van verhoogde rechten    |
|----------------|------|-------------------------------------|

Azure CycleCloud:
|----------------|------|-------------------------------------|
| CVE-ID         | CVSS | Impact                              |
|----------------|------|-------------------------------------|
```

```
| CVE-2026-77909 | 7,70 | Toegang tot gevoelige gegevens      |
|----------------|------|-------------------------------------|

Azure Resource Manager (ARM):
|----------------|------|-------------------------------------|
| CVE-ID         | CVSS | Impact                              |
|----------------|------|-------------------------------------|
| CVE-2026-81961 | 9,90 | 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

Referenties

- https://portal.msrc.microsoft.com/en-us/security-guidance

Kwetsbaarheden

CVE	CVSS Score
CVE-2026-62895	
CVE-2026-69854	
CVE-2026-77909	
CVE-2026-81961	

CWE's

CWE	Beschrijving
CWE-22	

Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	
CWE-89	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')
CWE-522	Insufficiently Protected Credentials
CWE-942	Permissive Cross-domain Security Policy with Untrusted Domains
CWE-1390	Weak Authentication

Getroffen producten

Microsoft
Azure Arc SQL Server Extension
Azure CycleCloud 8.9.2
Azure Resource Manager
Spring Cloud Azure

Disclaimer