Nationaal Cyber Security Centrum
Ministerie van Justitie en Veiligheid

NCSC-2026-0009

Kwetsbaarheden verholpen in Microsoft Azure

NCSC Advisory
Prioriteit: Normaal
Gepubliceerd op: 13-01-2026

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 kwetsbaarheden verholpen in diverse Azure-componenten.

Duiding

Een kwaadwillende kan de kwetsbaarheden misbruiken om zich verhoogde rechten toe te kennen en zo toegang te krijgen tot gevoelige gegevens of code uit te voeren waartoe de kwaadwillende aanvankelijk niet is geautoriseerd.

Voor succesvol misbruik moet de kwaadwillende over voorafgaande authenticatie beschikken in het kwetsbare systeem.

```
Azure Connected Machine Agent:
|----------------|------|-------------------------------------|
| CVE-ID         | CVSS | Impact                              |
|----------------|------|-------------------------------------|
| CVE-2026-21224 | 7.80 | Verkrijgen van verhoogde rechten    |
|----------------|------|-------------------------------------|

Windows Admin Center:
|----------------|------|-------------------------------------|
| CVE-ID         | CVSS | Impact                              |
|----------------|------|-------------------------------------|
| CVE-2026-20965 | 7.50 | Verkrijgen van verhoogde rechten    |
|----------------|------|-------------------------------------|

Azure Core shared client library for Python:
|----------------|------|-------------------------------------|
| CVE-ID         | CVSS | Impact                              |
|----------------|------|-------------------------------------|
| CVE-2026-21226 | 7.50 | 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

Kwetsbaarheden

CVE	CVSS Score
CVE-2026-20965	7.5 HIGH
CVE-2026-21224	7.8 HIGH
CVE-2026-21226	7.5 HIGH

CWE's

CWE	Beschrijving
CWE-121	Stack-based Buffer Overflow
CWE-347	Improper Verification of Cryptographic Signature
CWE-502	Deserialization of Untrusted Data

Getroffen producten

Microsoft
Azure Connected Machine Agent
Azure Core shared client library for Python
Windows Admin Center in Azure Portal

Disclaimer