Nationaal Cyber Security Centrum
Ministerie van Justitie en Veiligheid

NCSC-2026-0142

Kwetsbaarheden verholpen in Microsoft Azure

NCSC Advisory
Prioriteit: Normaal
Gepubliceerd op: 12-05-2026

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 voor te doen als andere gebruiker, zich verhoogde rechten toe te kennen, willekeurige code uit te voeren en mogelijk daarmee toegang te krijgen tot gevoelige gegevens.

De kwetsbaarheden met kenmerk CVE-2026-40379, CVE-2026-32207, CVE-2026-33109, CVE-2026-33844, CVE-2026-34327, CVE-2026-35428, CVE-2026-35435 en CVE-2026-41105 zijn reeds centraal verholpen door Microsoft en slechts opgenomen ter informatie. Voor deze kwetsbaarheden zijn geen acties benodigd.

Azure Machine Learning:

CVE-ID	CVSS	Impact
CVE-2026-32207	8.80	Voordoen als andere gebruiker
CVE-2026-33833	8.20	Voordoen als andere gebruiker

Azure Monitor Agent:

CVE-ID	CVSS	Impact
CVE-2026-32204	7.80	Verkrijgen van verhoogde rechten
CVE-2026-42830	6.50	Verkrijgen van verhoogde rechten

Microsoft Partner Center:

CVE-ID	CVSS	Impact
CVE-2026-34327	8.20	Voordoen als andere gebruiker

Azure Connected Machine Agent:

CVE-ID	CVSS	Impact

CVE-2026-40381	7.80	Verkrijgen van verhoogde rechten

Azure SDK:

CVE-ID	CVSS	Impact
CVE-2026-33117	9.10	Omzeilen van beveiligingsmaatregel

Microsoft SSO Plugin for Jira & Confluence:

CVE-ID	CVSS	Impact
CVE-2026-41103	9.10	Verkrijgen van verhoogde rechten

Azure Notification Service:

CVE-ID	CVSS	Impact
CVE-2026-41105	8.10	Verkrijgen van verhoogde rechten

Azure Logic Apps:

CVE-ID	CVSS	Impact
CVE-2026-42823	9.90	Verkrijgen van verhoogde rechten

Azure Entra ID:

CVE-ID	CVSS	Impact
CVE-2026-40379	9.30	Voordoen als andere gebruiker

Windows Admin Center:

CVE-ID	CVSS	Impact

```
|----------------|------|-------------------------------------|
| CVE-2026-41086 | 8.80 | Verkrijgen van verhoogde rechten    |
|----------------|------|-------------------------------------|

Azure AI Foundry M365 published agents:
|----------------|------|-------------------------------------|
| CVE-ID         | CVSS | Impact                              |
|----------------|------|-------------------------------------|
| CVE-2026-35435 | 8.60 | Verkrijgen van verhoogde rechten    |
|----------------|------|-------------------------------------|

Azure Cloud Shell:
|----------------|------|-------------------------------------|
| CVE-ID         | CVSS | Impact                              |
|----------------|------|-------------------------------------|
| CVE-2026-35428 | 9.60 | Voordoen als andere gebruiker       |
|----------------|------|-------------------------------------|

Azure Managed Instance for Apache Cassandra:
|----------------|------|-------------------------------------|
| CVE-ID         | CVSS | Impact                              |
|----------------|------|-------------------------------------|
| CVE-2026-33109 | 9.90 | Uitvoeren van willekeurige code     |
| CVE-2026-33844 | 9.00 | 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-2026-40379	5.3 MEDIUM
CVE-2026-32207	8.8 HIGH

CVE-2026-33833	8.2 HIGH
CVE-2026-33109	9.9 CRITICAL
CVE-2026-33844	9.0 CRITICAL
CVE-2026-32204	7.8 HIGH
CVE-2026-33117	9.1 CRITICAL
CVE-2026-41086	8.8 HIGH
CVE-2026-40381	7.8 HIGH
CVE-2026-41103	9.1 CRITICAL
CVE-2026-42823	9.9 CRITICAL
CVE-2026-42830	6.5 MEDIUM
CVE-2026-34327	8.2 HIGH
CVE-2026-35428	9.6 CRITICAL
CVE-2026-35435	8.6 HIGH
CVE-2026-41105	8.1 HIGH

CWE's

CWE	Beschrijving
CWE-20	Improper Input Validation
CWE-73	External Control of File Name or Path
CWE-74	Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')
CWE-77	Improper Neutralization of Special Elements used in a Command ('Command Injection')
CWE-79	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')

CWE-200	Exposure of Sensitive Information to an Unauthorized Actor
CWE-284	Improper Access Control
CWE-287	Improper Authentication
CWE-303	Incorrect Implementation of Authentication Algorithm
CWE-347	Improper Verification of Cryptographic Signature
CWE-426	Untrusted Search Path
CWE-610	Externally Controlled Reference to a Resource in Another Sphere
CWE-918	Server-Side Request Forgery (SSRF)

Getroffen producten

Microsoft
Azure
Azure AI Foundry
Azure Cloud Shell
Azure Connected Machine Agent
Azure Logic Apps
Azure Machine Learning
Azure Managed Instance for Apache Cassandra
Azure Monitor Action Group notification system
Azure Monitor Agent

Azure Monitor Agent Metrics Extension
Azure SDK for Java
Microsoft Confluence SAML SSO plugin
Microsoft Enterprise Security Token Service (ESTS)
Microsoft JIRA SAML SSO plugin
Microsoft Partner Center
Windows Admin Center in Azure Portal

Disclaimer