Nationaal Cyber Security Centrum
*Ministerie van Justitie en Veiligheid*

# NCSC-2026-0287

## Kwetsbaarheden verholpen in Microsoft Azure

NCSC Security Advisory
Prioriteit: Normaal
Gepubliceerd op: 12-08-2026

**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 aanvallen uit te voeren die kunnen leiden tot de categorieën schade zoals benoemd in onderstaande tabel.

De kwetsbaarheid met kenmerk **CVE-2026-56162**, met een CVSS score van 10.0 en de kwetsbaarheden met kenmerk **CVE-2026-50516, CVE-2026-56161, CVE-2026-59115, CVE-2026-62830, CVE-2026-62873** en **CVE-2026-68823**, elk met een CVSS score hoger dan 9, zijn reeds centraal verholpen door Microsoft zelf en slechts opgenomen ter informatie. Hiervoor zijn geen acties vereist.

De kwetsbaarheid met kenmerk **CVE-2026-50481**, met een CVSS score van 9.9 echter, vereist **wel** actie. Deze kwetsbaarheid bevindt zich in de Azure Active Directory en stelt een kwaadwillende in staat om zich verhoogde rechten toe te kennen en daarmee toegang te krijgen tot gegevens en componenten waartoe de kwaadwillende aanvankelijk niet is geautoriseerd.

```
Azure Monitor Agent:
|----------------|------|-------------------------------------|
| CVE-ID         | CVSS | Impact                              |
|----------------|------|-------------------------------------|
| CVE-2026-47299 | 7.20 | Verkrijgen van verhoogde rechten    |
|----------------|------|-------------------------------------|

Microsoft Purview eDiscovery:
|----------------|------|-------------------------------------|
| CVE-ID         | CVSS | Impact                              |
|----------------|------|-------------------------------------|
| CVE-2026-65668 | 8.80 | Verkrijgen van verhoogde rechten    |
|----------------|------|-------------------------------------|

Microsoft Azure Kubernetes Service:
|----------------|------|-------------------------------------|
| CVE-ID         | CVSS | Impact                              |
|----------------|------|-------------------------------------|
| CVE-2026-50516 | 9.40 | Verkrijgen van verhoogde rechten    |
|----------------|------|-------------------------------------|

Azure Entra ID:
|----------------|------|-------------------------------------|
```

| CVE-ID | CVSS | Impact |
|---|---|---|
| CVE-2026-62869 | 8.80 | Voordoen als andere gebruiker |

Microsoft Entra Connect Sync:

| CVE-ID | CVSS | Impact |
|---|---|---|
| CVE-2026-65673 | 7.80 | Verkrijgen van verhoogde rechten |

Azure SQL Database:

| CVE-ID | CVSS | Impact |
|---|---|---|
| CVE-2026-63522 | 7.80 | Verkrijgen van verhoogde rechten |
| CVE-2026-56162 | 10.0 | Verkrijgen van verhoogde rechten |

Azure Logic Apps:

| CVE-ID | CVSS | Impact |
|---|---|---|
| CVE-2026-56161 | 9.60 | Toegang tot gevoelige gegevens |

Azure Active Directory:

| CVE-ID | CVSS | Impact |
|---|---|---|
| CVE-2026-50481 | 9.90 | Verkrijgen van verhoogde rechten |

Application Insights Profiler:

| CVE-ID | CVSS | Impact |
|---|---|---|
| CVE-2026-49163 | 8.80 | Verkrijgen van verhoogde rechten |

Azure SRE Agent:

| CVE-ID | CVSS | Impact |
|---|---|---|
| CVE-2026-62830 | 9.90 | Verkrijgen van verhoogde rechten |

Microsoft Entra Provisioning Service (SyncFabric):

| CVE-ID | CVSS | Impact |
|---|---|---|
| CVE-2026-59115 | 9.90 | Verkrijgen van verhoogde rechten |

Azure CycleCloud:

| CVE-ID | CVSS | Impact |
|---|---|---|
| CVE-2026-70340 | 8.10 | Verkrijgen van verhoogde rechten |
| CVE-2026-65806 | 6.50 | Toegang tot gevoelige gegevens |

Azure Confidential Ledger:

| CVE-ID | CVSS | Impact |
|---|---|---|
| CVE-2026-68823 | 9.10 | Uitvoeren van willekeurige code |

Microsoft 365 Admin Center:

| CVE-ID | CVSS | Impact |
|---|---|---|
| CVE-2026-62873 | 9.80 | Verkrijgen van verhoogde rechten |

Azure Storage Explorer:

| CVE-ID | CVSS | Impact |
|---|---|---|
| CVE-2026-57104 | 8.80 | 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

## Kwetsbaarheden

| CVE | CVSS Score |
|---|---|
| CVE-2026-65668 | 8.8 HIGH |
| CVE-2026-59115 | 9.9 CRITICAL |
| CVE-2026-50481 | 9.9 CRITICAL |
| CVE-2026-62873 | 9.8 CRITICAL |
| CVE-2026-47299 | 7.2 HIGH |
| CVE-2026-70340 | 8.1 HIGH |
| CVE-2026-65806 | 6.5 MEDIUM |
| CVE-2026-65673 | 7.8 HIGH |
| CVE-2026-63522 | 7.8 HIGH |
| CVE-2026-56162 | 10.0 CRITICAL |
| CVE-2026-62830 | 9.9 CRITICAL |
| CVE-2026-56161 | 9.6 CRITICAL |
| CVE-2026-50516 | 9.4 CRITICAL |
| CVE-2026-49163 | 8.8 HIGH |

| | |
|---|---|
| CVE-2026-68823 | 9.1 CRITICAL |
| CVE-2026-62869 | 8.8 HIGH |
| CVE-2026-57104 | 8.8 HIGH |

## CWE's

| CWE | Beschrijving |
|---|---|
| CWE-22 | Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') |
| CWE-35 | Path Traversal: '.../...//' |
| 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-89 | Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') |
| CWE-269 | Improper Privilege Management |
| CWE-284 | Improper Access Control |
| CWE-287 | Improper Authentication |
| CWE-306 | Missing Authentication for Critical Function |
| CWE-345 | Insufficient Verification of Data Authenticity |
| CWE-347 | Improper Verification of Cryptographic Signature |
| CWE-471 | Modification of Assumed-Immutable Data (MAID) |
| CWE-732 | Incorrect Permission Assignment for Critical Resource |
| CWE-749 | Exposed Dangerous Method or Function |
| CWE-862 | Missing Authorization |

## Getroffen producten

| **Microsoft** |
| --- |
| Application Insights<br>Profiler |
| Azure |
| Azure Active<br>Directory |
| Azure Confidential<br>Ledger |
| Azure CycleCloud<br>8.9.1 |
| Azure CycleCloud<br>8.9.2 |
| Azure Kubernetes<br>Service |
| Azure Logic<br>Apps |
| Azure Monitor Agent Linux<br>Extension |
| Azure SQL<br>Database |
| Azure SRE<br>Agent |
| Azure Storage<br>Explorer |
| Entra |
| Microsoft 365 Admin<br>Center |
| Microsoft Entra<br>Connect |

| |
|---|
| Microsoft Entra ID |
| Microsoft Entra Provisioning Service |
| Microsoft Purview eDiscovery |
| Windows Admin Center |

## Disclaimer