Nationaal Cyber Security Centrum
Ministerie van Justitie en Veiligheid

NCSC-2026-0183

Kwetsbaarheden verholpen in Microsoft Azure

NCSC Security Advisory
Prioriteit: Normaal
Gepubliceerd op: 09-06-2026

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

De ernstigste kwetsbaarheid bevond zich in HorizonDB en heeft kenmerk CVE-2026-48567 toegewezen gekregen. Deze kwetsbaarheid is reeds door Microsoft centraal verholpen en vereist geen verdere acties. Deze kwetsbaarheid is ter informatie opgenomen.

```
Microsoft Graph:
|----------------|------|-------------------------------------|
| CVE-ID         | CVSS | Impact                              |
|----------------|------|-------------------------------------|
| CVE-2026-47655 | 6.50 | Toegang tot gevoelige gegevens      |
|----------------|------|-------------------------------------|

Azure Stack Edge:
|----------------|------|-------------------------------------|
| CVE-ID         | CVSS | Impact                              |
|----------------|------|-------------------------------------|
| CVE-2026-41098 | 8.40 | Voordoen als andere gebruiker       |
| CVE-2026-47643 | 9.80 | Uitvoeren van willekeurige code     |
|----------------|------|-------------------------------------|

Microsoft Azure Kubernetes Service:
|----------------|------|-------------------------------------|
| CVE-ID         | CVSS | Impact                              |
|----------------|------|-------------------------------------|
| CVE-2026-32193 | 8.80 | Uitvoeren van willekeurige code     |
|----------------|------|-------------------------------------|

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

```
| CVE-2026-48567 | 10.00 | 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-2026-32193	8.8 HIGH
CVE-2026-41098	8.4 HIGH
CVE-2026-47643	9.8 CRITICAL
CVE-2026-47655	6.5 MEDIUM
CVE-2026-48567	6.9 MEDIUM

CWE's

CWE	Beschrijving
CWE-22	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')
CWE-73	External Control of File Name or Path
CWE-79	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')
CWE-200	Exposure of Sensitive Information to an Unauthorized Actor
CWE-290	Authentication Bypass by Spoofing

Getroffen producten

Microsoft
Azure
Azure HorizonDB
Azure Kubernetes Service
Azure Stack Edge
Microsoft Graph

Disclaimer

The Netherlands Cyber Security Center (henceforth: NCSC-NL) maintains this page to enhance access to its information and security advisories. The use of this security advisory is subject to the following terms and conditions: NCSC-NL makes every reasonable effort to ensure that the content of this page is kept up to date, and that it is accurate and complete. Nevertheless, NCSC-NL cannot entirely rule out the possibility of errors, and therefore cannot give any warranty in respect of its completeness, accuracy or continuous keeping up-to-date. The information contained in this security advisory is intended solely for the purpose of providing general information to professional users. No rights can be derived from the information provided therein. NCSC-NL and the Kingdom of the Netherlands assume no legal liability or responsibility for any damage resulting from either the use or inability of use of this security advisory. This includes damage resulting from the inaccuracy of incompleteness of the information contained in the advisory. This security advisory is subject to Dutch law. All disputes related to or arising from the use of this advisory will be submitted to the competent court in The Hague. This choice of means also applies to the court in summary proceedings.