Nationaal Cyber Security Centrum
Ministerie van Justitie en Veiligheid

Advisory NCSC-2026-0475

PRIORITEIT: NORMAAL

Kwetsbaarheden verholpen in Microsoft Azure

Publicatiedatum: 10-11-2026

Toegestane verspreiding: TLP:WHITE
(Traffic Light Protocol)

Deze publicatie bevat het label TLP:WHITE en wordt door het Nationaal Cyber Security Center (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 de-len. Dit staat beschreven in de standaard First (www.first.org/tlp).

Ontvangers van TLP:WHITE mogen de informatie publiek verspreiden.

Reacties zijn welkom op info@ncsc.nl.

Feiten

Microsoft heeft meerdere 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-2026-119990, met een CVSS-score van 9.8 betreft ontbrekende authenticatie voor een kritieke functie in Azure OpenAI. Een ongeautoriseerde kwaadwillende kan deze kwetsbaarheid via het netwerk misbruiken om verhoogde rechten te verkrijgen. Voor de kwetsbaarheid met kenmerk CVE-2026-114162, met een CVSS-score van 9.1 geldt dat een geautoriseerde kwaadwillende door onvoldoende autorisatiecontroles in Microsoft Graph via het netwerk verhoogde rechten kan verkrijgen voor Microsoft Azure.

Azure File Sync:

CVE-ID	CVSS	Impact
CVE-2026-118288	7,00	Verkrijgen van verhoogde rechten

Azure Managed Grafana:

CVE-ID	CVSS	Impact
CVE-2026-114160	onb.	Verkrijgen van verhoogde rechten

Azure Local:

CVE-ID	CVSS	Impact
CVE-2026-105734	7,00	Verkrijgen van verhoogde rechten

Azure OpenAI:

CVE-ID	CVSS	Impact
CVE-2026-119990	9,80	Verkrijgen van verhoogde rechten

Microsoft Graph:

CVE-ID	CVSS	Impact
CVE-2026-114162	9,10	Verkrijgen van verhoogde rechten

Azure CycleCloud:

CVE-ID	CVSS	Impact
CVE-2026-102224	8,40	Verkrijgen van verhoogde rechten
CVE-2026-113822	6,50	Verkrijgen van verhoogde rechten
CVE-2026-113823	7,50	Toegang tot gevoelige gegevens
CVE-2026-114161	7,80	Verkrijgen van verhoogde rechten

Azure Front Door (AFD):

CVE-ID	CVSS	Impact
CVE-2026-118742	8,60	Verkrijgen van verhoogde rechten

Microsoft Entra Private Network Connector:

CVE-ID	CVSS	Impact
CVE-2026-109460	5,50	Toegang tot gevoelige gegevens

Microsoft Authentication Library for JavaScript:

CVE-ID	CVSS	Impact
CVE-2026-108469	6,80	Voordoen als andere gebruiker

Azure Firmware:

CVE-ID	CVSS	Impact
CVE-2026-109462	4,40	Omzeilen van beveiligingsmaatregel

Azure CLI:

CVE-ID	CVSS	Impact
CVE-2026-109457	8,00	Uitvoeren van willekeurige code

Microsoft Authentication Library (MSAL) for Node.js:

CVE-ID	CVSS	Impact
CVE-2026-108470	onb.	Toegang tot gevoelige gegevens

Microsoft Authentication Library (MSAL) for .NET:

```
Azure Pipelines:
|------------------|------|-------------------------------------|
| CVE-ID           | CVSS | Impact                              |
|------------------|------|-------------------------------------|
| CVE-2026-119989  | 8,20 | Uitvoeren van willekeurige code     |
|------------------|------|-------------------------------------|


Azure NFS mount helper (aznfs):
|------------------|------|-------------------------------------|
| CVE-ID           | CVSS | Impact                              |
|------------------|------|-------------------------------------|
| CVE-2026-105494  | onb. | 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-2026-85923	8.8 HIGH
CVE-2026-102224	8.4 HIGH
CVE-2026-105494	7.8 HIGH
CVE-2026-105734	7.0 HIGH
CVE-2026-109457	8.0 HIGH

CVE	CVSS Score
CVE-2026-109462	4.4 MEDIUM
CVE-2026-109467	9.9 CRITICAL
CVE-2026-112745	6.5 MEDIUM
CVE-2026-113822	6.5 MEDIUM
CVE-2026-113823	7.5 HIGH
CVE-2026-114160	9.8 CRITICAL
CVE-2026-114161	7.8 HIGH
CVE-2026-118288	7.0 HIGH
CVE-2026-118742	8.6 HIGH
CVE-2026-119989	8.2 HIGH
CVE-2026-119990	9.8 CRITICAL
CVE-2026-120783	6.4 MEDIUM
CVE-2026-121668	7.7 HIGH
CVE-2026-122986	7.8 HIGH

CWE's

CWE	Beschrijving
CWE-22	Improper Limitation of a Pathname to a Restricted Directory
CWE-77	Improper Neutralization of Special Elements used in a Command
CWE-78	Improper Neutralization of Special Elements used in an OS Command
CWE-79	Improper Neutralization of Input During Web Page Generation
CWE-299	Improper Check for Certificate Revocation
CWE-306	Missing Authentication for Critical Functionality
CWE-426	Untrusted Search Path
CWE-488	Exposure of Data Element to Wrong Session
CWE-522	Insufficiently Protected Credentials
CWE-732	Incorrect Permission Assignment for Critical Resource

CWE	Beschrijving
CWE-862	Missing Authorization
CWE-863	Incorrect Authorization

Getroffen producten

Microsoft
@azure/msal-node
Azure CycleCloud 8.9.1
Azure CycleCloud 8.9.2
Azure CycleCloud 8.9.2 on Linux
Azure File Sync v21
Azure File Sync v22
Azure File Sync v23
Azure Front Door
Azure Identity SDK for Java
Azure Local on Azure Linux 3.0
Azure Machine Learning
Azure Managed Grafana
Azure Open AI
Azure Privileged Identity Management (PIM)
Azure Virtual Machines
Azure Web Apps
Microsoft Authentication Library (MSAL) for .NET on Windows
Microsoft Authentication Library for JavaScript
Microsoft Entra Private Network Connector
Microsoft Identity Manager

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.