



NCSC-2026-0057

Kwetsbaarheden verholpen in Microsoft Azure

NCSC Advisory

Prioriteit: Normaal

Gepubliceerd op: 10-02-2026

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 mogelijk verhoogde rechten toe te kennen en zo willekeurige code uit te voeren of toegang te krijgen tot gevoelige gegevens.

Van de kwetsbaarheden met kenmerk CVE-2026-21532, CVE-2026-24300 en CVE-2026-24302 meldt Microsoft dat deze in hun centrale Azure-infrastructuur zijn verholpen en dat deze kwetsbaarheden geen actie van gebruikers vereist. Deze kwetsbaarheden zijn ter informatie opgenomen.

Azure Front Door (AFD):

CVE-ID	CVSS	Impact
CVE-2026-24300	9.80	Verkrijgen van verhoogde rechten

Azure Function:

CVE-ID	CVSS	Impact
CVE-2026-21532	8.20	Toegang tot gevoelige gegevens

Azure HDInsights:

CVE-ID	CVSS	Impact
CVE-2026-21529	5.70	Voordoen als andere gebruiker

Azure Compute Gallery:

CVE-ID	CVSS	Impact
CVE-2026-23655	6.50	Toegang tot gevoelige gegevens
CVE-2026-21522	6.70	Verkrijgen van verhoogde rechten

|-----|-----|-----|

Azure Local:

CVE-ID	CVSS	Impact
CVE-2026-21228	8.10	Uitvoeren van willekeurige code

Azure Arc:

CVE-ID	CVSS	Impact
CVE-2026-24302	8.60	Verkrijgen van verhoogde rechten

Azure IoT SDK:

CVE-ID	CVSS	Impact
CVE-2026-21528	6.50	Toegang tot gevoelige gegevens

Azure DevOps Server:

CVE-ID	CVSS	Impact
CVE-2026-21512	6.50	Voordoen als andere gebruiker

Azure SDK:

CVE-ID	CVSS	Impact
CVE-2026-21531	9.80	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-2026-21512	6.5 MEDIUM
> CVE-2026-23655	6.5 MEDIUM
> CVE-2026-21522	6.7 MEDIUM
> CVE-2026-24300	9.3 CRITICAL
> CVE-2026-24302	6.9 MEDIUM
> CVE-2026-21532	6.9 MEDIUM
> CVE-2026-21528	6.5 MEDIUM
> CVE-2026-21531	9.8 CRITICAL
> CVE-2026-21529	5.7 MEDIUM
> CVE-2026-21228	8.1 HIGH

CWE's

CWE	Beschrijving
> 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-295	Improper Certificate Validation
➤ CWE-312	Cleartext Storage of Sensitive Information
➤ CWE-502	Deserialization of Untrusted Data
➤ CWE-918	Server-Side Request Forgery (SSRF)
➤ CWE-1327	Binding to an Unrestricted IP Address

Getroffen producten

Microsoft
Azure
Azure AI Language Authoring
Azure ARC
Azure DevOps Server 2022
Azure Front Door
Azure Functions
Azure HDInsight
Azure IoT Explorer
Azure Local
Microsoft ACI Confidential Containers

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.