Nationaal Cyber Security Centrum
Ministerie van Justitie en Veiligheid

NCSC-2026-0082

Kwetsbaarheden verholpen in Microsoft Azure

NCSC Advisory
Prioriteit: Normaal
Gepubliceerd op: 10-03-2026

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 kwetbaarheden verholpen in diverse Azure componenten.

Duiding

Een kwadwillende kan de kwetsbaarheden misbruiken om zich voor te doen als andere gebruiker, zich verhoogde rechten toe te kennen of toegang te krijgen tot gevoelige gegevens.

Azure Entra ID:

CVE-ID	CVSS	Impact
CVE-2026-26148	8.10	Verkrijgen van verhoogde rechten

Azure IoT Explorer:

CVE-ID	CVSS	Impact
CVE-2026-23664	7.50	Toegang tot gevoelige gegevens
CVE-2026-26121	7.50	Voordoen als andere gebruiker
CVE-2026-23661	7.50	Toegang tot gevoelige gegevens
CVE-2026-23662	7.50	Toegang tot gevoelige gegevens

Azure Portal Windows Admin Center:

CVE-ID	CVSS	Impact
CVE-2026-23660	7.80	Verkrijgen van verhoogde rechten

Azure Compute Gallery:

CVE-ID	CVSS	Impact
CVE-2026-23651	6.70	Verkrijgen van verhoogde rechten
CVE-2026-26124	6.70	Verkrijgen van verhoogde rechten
CVE-2026-26122	6.50	Toegang tot gevoelige gegevens

Azure MCP Server:

CVE-ID	CVSS	Impact
CVE-2026-26118	8.80	Verkrijgen van verhoogde rechten

Azure Linux Virtual Machines:

CVE-ID	CVSS	Impact
CVE-2026-23665	7.80	Verkrijgen van verhoogde rechten

Azure Windows Virtual Machine Agent:

CVE-ID	CVSS	Impact
CVE-2026-26117	7.80	Verkrijgen van verhoogde rechten

Azure Arc:

CVE-ID	CVSS	Impact
CVE-2026-26141	7.80	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

Dreigingsinformatie

CVE's toe te voegen:

CVE-2026-23651, CVE-2026-23660, CVE-2026-23661, CVE-2026-23662, CVE-2026-23664, CVE-2026-23665, CVE-2026-26117, CVE-2026-26118, CVE-2026-26121, CVE-2026-26122, CVE-2026-26124, CVE-2026-26141, CVE-2026-26148

Kwetsbaarheden

CVE	CVSS Score
CVE-2026-23651	6.7 MEDIUM
CVE-2026-23660	7.8 HIGH
CVE-2026-23661	7.5 HIGH
CVE-2026-23662	7.5 HIGH
CVE-2026-23664	7.5 HIGH
CVE-2026-23665	7.8 HIGH
CVE-2026-26117	7.8 HIGH
CVE-2026-26118	8.8 HIGH
CVE-2026-26121	7.5 HIGH
CVE-2026-26122	6.5 MEDIUM
CVE-2026-26124	6.7 MEDIUM
CVE-2026-26141	7.8 HIGH
CVE-2026-26148	8.1 HIGH

CWE's

CWE	Beschrijving
CWE-20	Improper Input Validation
CWE-35	Path Traversal: '.../...//'
CWE-122	Heap-based Buffer Overflow

CWE-284	Improper Access Control
CWE-287	Improper Authentication
CWE-288	Authentication Bypass Using an Alternate Path or Channel
CWE-306	Missing Authentication for Critical Function
CWE-319	Cleartext Transmission of Sensitive Information
CWE-625	Permissive Regular Expression
CWE-918	Server-Side Request Forgery (SSRF)
CWE-923	Improper Restriction of Communication Channel to Intended Endpoints
CWE-1188	Initialization of a Resource with an Insecure Default

Getroffen producten

Microsoft
Arc Enabled Servers - Azure Connected Machine Agent
Azure
Azure Automation Hybrid Worker Windows Extension
Azure IoT Explorer
Azure Linux Virtual Machines with Azure Diagnostics extension
Azure MCP Server Tools
Microsoft ACI Confidential Containers
Microsoft Azure AD SSH Login extension for Linux
Microsoft Azure Container Instances Confidential Containers

Windows Admin Center in
Azure Portal

Disclaimer