



Advisory NCSC-2026-0421

PRIORITEIT: NORMAAL

Kwetsbaarheden verholpen in Microsoft Azure

Publicatiedatum: 13-10-2026

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 delen. 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 kwetsbaarheden verholpen in diverse Azure componenten, zoals Key Vault, DevOps, API center en Storage.

Duiding

Een kwaadwillende kan de kwetsbaarheden misbruiken om beveiligingsmaatregelen te omzeilen, zich verhoogde rechten toe te kennen, willekeurige code uit te voeren en toegang te krijgen tot gevoelige gegevens.

De kwetsbaarheden met kenmerk CVE-2026-83943, CVE-2026-96207, CVE-2026-69435 en CVE-2026-83947 zijn reeds centraal door Microsoft verholpen en vereisen geen verdere acties. Deze zijn ter informatie opgenomen.

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-2026-85922	
CVE-2026-85925	
CVE-2026-88132	
CVE-2026-69877	
CVE-2026-83943	8.7 HIGH
CVE-2026-88094	
CVE-2026-100207	
CVE-2026-96207	10.0 CRITICAL

CVE	CVSS Score
CVE-2026-96205	
CVE-2026-96204	
CVE-2026-69435	9.6 CRITICAL
CVE-2026-83947	7.7 HIGH

CWE's

CWE	Beschrijving
CWE-78	Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')
CWE-295	Improper Certificate Validation
CWE-346	Origin Validation Error
CWE-862	Missing Authorization
CWE-918	Server-Side Request Forgery (SSRF)
CWE-923	Improper Restriction of Communication Channel to Intended Endpoints
CWE-1390	Weak Authentication

Getroffen producten

Microsoft
Arc Enabled Servers - Azure Connected Machine Agent
Azure
Azure API Center
Azure CLI
Azure Container Storage enabled by Azure Arc
Azure CycleCloud 8.9.1

Microsoft

Azure CycleCloud 8.9.2

Azure DevOps CLI Extension

Azure Event Grid System

Azure Key Vault Client SDK

Azure SRE Agent

Azure Storage Blobs client library for Java

Microsoft Bookings

Microsoft Partner Center

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 or 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.