



NCSC-2025-0249

Kwetsbaarheden verholpen in Azure-producten

NCSC Advisory

Prioriteit: Normaal

Gepubliceerd op: 13-08-2025

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 Azure-producten.

Duiding

De kwetsbaarheden zijn gerelateerd aan onjuiste toegangscontrolemechanismen, waardoor geautoriseerde aanvallers lokale spoofing-aanvallen kunnen uitvoeren, verhoogde privileges kunnen verkrijgen, gevoelige informatie kunnen onthullen en de integriteit van systemen kunnen compromitteren. Dit kan leiden tot ongeautoriseerde toegang en manipulatie van gevoelige gegevens.

Azure Stack:

CVE-ID	CVSS	Impact
CVE-2025-53765	4.40	Toegang tot gevoelige gegevens
CVE-2025-53793	7.50	Toegang tot gevoelige gegevens

Azure OpenAI:

CVE-ID	CVSS	Impact
CVE-2025-53767	10.00	Verkrijgen van verhoogde rechten

Azure Portal:

CVE-ID	CVSS	Impact
CVE-2025-53792	9.10	Verkrijgen van verhoogde rechten

Azure Virtual Machines:

CVE-ID	CVSS	Impact
CVE-2025-53781	7.70	Toegang tot gevoelige gegevens
CVE-2025-49707	7.90	Voordoen als andere gebruiker

Azure File Sync:

CVE-ID	CVSS	Impact
CVE-2025-53729	7.80	Verkrijgen van verhoogde rechten

Oplossingen

Microsoft heeft updates uitgebracht om de kwetsbaarheden te verhelpen. Zie bijgevoegde referenties voor meer informatie.

Referenties

> <https://portal.msrc.microsoft.com/en-us/security-guidance>

Kwetsbaarheden

CVE	CVSS Score
> CVE-2025-49707	7.9 HIGH
> CVE-2025-53729	
> CVE-2025-53765	
> CVE-2025-53767	6.9 MEDIUM
> CVE-2025-53781	7.7 HIGH
> CVE-2025-53792	6.9 MEDIUM
> CVE-2025-53793	

CWE's

CWE	Beschrijving
> CVE-359	Exposure of Private Personal Information to an Unauthorized Actor
> CVE-284	Improper Access Control

➤ CWE-22	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')
➤ CWE-200	Exposure of Sensitive Information to an Unauthorized Actor
➤ CWE-287	Improper Authentication

Getroffen producten

Microsoft
Azure
Azure File Sync
Azure Stack Hub
Azure File Sync v18
Azure File Sync v19
Azure File Sync v20
Azure File Sync v21
Azure Open AI
Azure Portal
Azure Stack Hub 2406

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.