Nationaal Cyber Security Centrum
Ministerie van Justitie en Veiligheid

NCSC-2025-0156

Kwetsbaarheden verholpen in Microsoft Azure

NCSC Advisory
Prioriteit: Normaal
Gepubliceerd op: 13-05-2025

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 diverse Azure componenten.

Duiding

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

Microsoft heeft inmiddels updates uitgebracht om de kwetsbaarheden te verhelpen met kenmerk CVE-2025-47733, CVE-2025-29972, CVE-2025-29827 en CVE-2025-33072. Deze kwetsbaarheden bevinden zich in online componenten en vereisen geen verdere actie.

Azure Automation:

CVE-ID	CVSS	Impact
CVE-2025-29827	9.90	Verkrijgen van verhoogde rechten

Azure:

CVE-ID	CVSS	Impact
CVE-2025-30387	9.80	Verkrijgen van verhoogde rechten
CVE-2025-33072	8.10	Toegang tot gevoelige gegevens

Azure Storage Resource Provider:

CVE-ID	CVSS	Impact
CVE-2025-29972	9.90	Voordoen als andere gebruiker

Microsoft Power Apps:

CVE-ID	CVSS	Impact
CVE-2025-47733	9.10	Toegang tot gevoelige gegevens

```
Windows Hardware Lab Kit:
|----------------|------|-------------------------------------|
| CVE-ID         | CVSS | Impact                              |
|----------------|------|-------------------------------------|
| CVE-2025-27488 | 6.70 | Verkrijgen van verhoogde rechten    |
|----------------|------|-------------------------------------|

Azure File Sync:
|----------------|------|-------------------------------------|
| CVE-ID         | CVSS | Impact                              |
|----------------|------|-------------------------------------|
| CVE-2025-29973 | 7.00 | 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

Kwetsbaarheden

CVE	CVSS Score
CVE-2025-29973	7.0 HIGH
CVE-2025-30387	
CVE-2025-33072	8.1 HIGH
CVE-2025-27488	
CVE-2025-29972	9.9 CRITICAL
CVE-2025-29827	9.9 CRITICAL
CVE-2025-47733	9.1 CRITICAL

CWE's

CWE	Beschrijving
CWE-798	Use of Hard-coded Credentials
CWE-285	Improper Authorization
CWE-284	Improper Access Control
CWE-918	Server-Side Request Forgery (SSRF)
CWE-22	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')

Getroffen producten

Microsoft
Windows HLK for Windows Server 2019
Windows HLK for Windows 10 version 2004
Windows 10 HLK version 21H2
Windows 10 HLK Version 22H2
Windows HLK for Windows Server 2022
Windows 10 HLK version 20H2
Windows 11 HLK 22H2
Windows 10 HLK version 21H1
Windows 10 HLK Version 1809

Windows 11 HLK 24H2
Windows HLK for Windows Server 2025
Azure Automation
Azure Storage Resource Provider (SRP)
Azure File Sync v20.0
Azure File Sync v19.0
Microsoft msagsfeedback.azurewebsites.net
Microsoft Power Apps

Disclaimer