Nationaal Cyber Security Centrum
Ministerie van Justitie en Veiligheid

NCSC-2025-0311

Kwetsbaarheden verholpen in Microsoft Azure

NCSC Advisory
Prioriteit: Normaal
Gepubliceerd op: 14-10-2025

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

De ernstigste kwetsbaarheden bevinden zich in Azure Entra ID en stellen een kwaadwillende in staat om zich verhoogde rechten toe te kennen. Deze kwetsbaarheden bevinden zich in een centrale component van Azure en zijn inmiddels verholpen. Voor deze kwetsbaarheden is verder geen actie benodigd en deze zijn opgenomen ter informatie.

```
Azure Connected Machine Agent:
|----------------|------|-------------------------------------|
| CVE-ID         | CVSS | Impact                              |
|----------------|------|-------------------------------------|
| CVE-2025-47989 | 7.00 | Verkrijgen van verhoogde rechten    |
| CVE-2025-58724 | 7.80 | Verkrijgen van verhoogde rechten    |
|----------------|------|-------------------------------------|

Azure Entra ID:
|----------------|------|-------------------------------------|
| CVE-ID         | CVSS | Impact                              |
|----------------|------|-------------------------------------|
| CVE-2025-59218 | 9.60 | Verkrijgen van verhoogde rechten    |
| CVE-2025-59246 | 9.80 | Verkrijgen van verhoogde rechten    |
|----------------|------|-------------------------------------|

Redis Enterprise:
|----------------|------|-------------------------------------|
| CVE-ID         | CVSS | Impact                              |
|----------------|------|-------------------------------------|
| CVE-2025-59271 | 8.70 | Verkrijgen van verhoogde rechten    |
|----------------|------|-------------------------------------|

Confidential Azure Container Instances:
|----------------|------|-------------------------------------|
| CVE-ID         | CVSS | Impact                              |
```

```
|----------------|------|-------------------------------------|
| CVE-2025-59291 | 8.20 | Verkrijgen van verhoogde rechten    |
| CVE-2025-59292 | 8.20 | Verkrijgen van verhoogde rechten    |
|----------------|------|-------------------------------------|

Azure Monitor Agent:
|----------------|------|-------------------------------------|
| CVE-ID         | CVSS | Impact                              |
|----------------|------|-------------------------------------|
| CVE-2025-59494 | 7.80 | Verkrijgen van verhoogde rechten    |
| CVE-2025-59285 | 7.00 | Verkrijgen van verhoogde rechten    |
|----------------|------|-------------------------------------|

Azure PlayFab:
|----------------|------|-------------------------------------|
| CVE-ID         | CVSS | Impact                              |
|----------------|------|-------------------------------------|
| CVE-2025-59247 | 8.80 | Verkrijgen van verhoogde rechten    |
|----------------|------|-------------------------------------|

Azure Monitor:
|----------------|------|-------------------------------------|
| CVE-ID         | CVSS | Impact                              |
|----------------|------|-------------------------------------|
| CVE-2025-55321 | 8.70 | Voordoen als andere gebruiker       |
|----------------|------|-------------------------------------|
```

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-2025-47989	7.0 HIGH

CVE-2025-59291	8.2 HIGH
CVE-2025-59292	8.2 HIGH
CVE-2025-59494	7.8 HIGH
CVE-2025-59285	7.0 HIGH
CVE-2025-58724	7.8 HIGH
CVE-2025-59218	5.3 MEDIUM
CVE-2025-59246	9.3 CRITICAL
CVE-2025-59247	8.7 HIGH
CVE-2025-59271	6.3 MEDIUM
CVE-2025-55321	4.8 MEDIUM

CWE's

CWE	Beschrijving
CWE-73	External Control of File Name or Path
CWE-79	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')
CWE-269	Improper Privilege Management
CWE-284	Improper Access Control
CWE-285	Improper Authorization
CWE-306	Missing Authentication for Critical Function
CWE-502	Deserialization of Untrusted Data
CWE-565	Reliance on Cookies without Validation and Integrity Checking

Getroffen producten

Microsoft
Arc Enabled Servers - Azure Connected Machine Agent
Azure Cache for Redis Enterprise
Azure Compute Gallery
Azure Managed Redis
Azure Monitor
Azure PlayFab
Microsoft Entra
Microsoft Entra ID

Disclaimer