



# 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](http://www.first.org/tlp)).

Ontvangers van TLP:WHITE mogen de informatie publiek verspreiden.

Uw reacties zijn welkom op [info@ncsc.nl](mailto: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   |
|----------------------------------|--------------|
| > <a href="#">CVE-2025-29973</a> | 7.0 HIGH     |
| > <a href="#">CVE-2025-30387</a> |              |
| > <a href="#">CVE-2025-33072</a> | 8.1 HIGH     |
| > <a href="#">CVE-2025-27488</a> |              |
| > <a href="#">CVE-2025-29972</a> | 9.9 CRITICAL |
| > <a href="#">CVE-2025-29827</a> | 9.9 CRITICAL |
| > <a href="#">CVE-2025-47733</a> | 9.1 CRITICAL |

## CWE's

| CWE                       | Beschrijving   |
|---------------------------|--|
| > <a href="#">CWE-798</a> | Use of Hard-coded Credentials  |
| > <a href="#">CWE-285</a> | Improper Authorization   |
| > <a href="#">CWE-284</a> | Improper Access Control  |
| > <a href="#">CWE-918</a> | Server-Side Request Forgery (SSRF)   |
| > <a href="#">CWE-22</a>  | 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<br>24H2                       |
| Windows HLK for Windows<br>Server 2025       |
| Azure<br>Automation                          |
| Azure Storage Resource<br>Provider (SRP)     |
| Azure File Sync<br>v20.0                     |
| Azure File Sync<br>v19.0                     |
| Microsoft<br>msagsfeedback.azurewebsites.net |
| Microsoft Power<br>Apps                      |

## 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.