



# NCSC-2025-0153

## Kwetsbaarheden verholpen in Microsoft Developer Tools

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 Developer Tools.

## Duiding

Een kwaadwillende kan de kwetsbaarheden misbruiken om aanvallen uit te voeren die kunnen leiden tot de volgende categorieën schade:

- Omzeilen van een beveiligingsmaatregel
- Uitvoer van willekeurige code (gebruikersrechten)
- Toegang tot gevoelige gegevens
- Spoofing
- Verkrijgen van verhoogde rechten

Voor de kwetsbaarheid met kenmerk CVE-2025-29813 heeft Microsoft inmiddels updates uitgerold binnen het Azure platform. Hiervoor zijn geen verdere acties nodig.

### Visual Studio:

CVE-ID	CVSS	Impact
CVE-2025-32703	5.50	Toegang tot gevoelige gegevens
CVE-2025-32702	7.80	Uitvoeren van willekeurige code

### .NET, Visual Studio, and Build Tools for Visual Studio:

CVE-ID	CVSS	Impact
CVE-2025-26646	8.00	Voordoens als andere gebruiker

### Visual Studio Code:

CVE-ID	CVSS	Impact
CVE-2025-21264	6.70	Omzeilen van beveiligingsmaatregel

### Azure DevOps:

CVE-ID	CVSS	Impact
--------	------	--------

CVE-ID	CVSS	Impact
CVE-2025-29813	10.00	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>

## Referenties

- <https://www.cve.org/CVERecord?id=CVE-2025-21264>
- <https://raw.githubusercontent.com/CVEProject/cvelistV5/main/cves/2025/21xxx/CVE-2025-21264.json>
- <https://www.cve.org/CVERecord?id=CVE-2025-29813>
- <https://raw.githubusercontent.com/CVEProject/cvelistV5/main/cves/2025/29xxx/CVE-2025-29813.json>
- <https://www.cve.org/CVERecord?id=CVE-2025-32702>
- <https://raw.githubusercontent.com/CVEProject/cvelistV5/main/cves/2025/32xxx/CVE-2025-32702.json>
- <https://www.cve.org/CVERecord?id=CVE-2025-32703>
- <https://raw.githubusercontent.com/CVEProject/cvelistV5/main/cves/2025/32xxx/CVE-2025-32703.json>
- <https://api.msrf.microsoft.com/cvrf/v3.0/cvrf/2025-May>

## Kwetsbaarheden

CVE	CVSS Score
➤ <a href="#">CVE-2025-26646</a>	
➤ <a href="#">CVE-2025-32703</a>	
➤ <a href="#">CVE-2025-32702</a>	
➤ <a href="#">CVE-2025-21264</a>	
➤ <a href="#">CVE-2025-29813</a>	<b>10.0 CRITICAL</b>

## CWE's

CWE	Beschrijving
> <a href="#">CWE-302</a>	Authentication Bypass by Assumed-Immutable Data
> <a href="#">CWE-1220</a>	Insufficient Granularity of Access Control
> <a href="#">CWE-77</a>	Improper Neutralization of Special Elements used in a Command ('Command Injection')
> <a href="#">CWE-552</a>	Files or Directories Accessible to External Parties
> <a href="#">CWE-200</a>	Exposure of Sensitive Information to an Unauthorized Actor
> <a href="#">CWE-73</a>	External Control of File Name or Path

## Getroffen producten

Microsoft
.NET 8.0 installed on Linux
.NET 8.0 installed on Mac OS
.NET 8.0 installed on Windows
.NET 9.0 installed on Linux
.NET 9.0 installed on Mac OS
.NET 9.0 installed on Windows
Azure DevOps
Build Tools for Visual Studio 2022

Microsoft Visual Studio 2017 version 15.9 (includes 15.0 - 15.8)
Microsoft Visual Studio 2019 version 16.11 (includes 16.0 - 16.10)
Microsoft Visual Studio 2022 version 17.10
Microsoft Visual Studio 2022 version 17.12
Microsoft Visual Studio 2022 version 17.13
Microsoft Visual Studio 2022 version 17.8
Visual Studio 2019
Visual Studio 2022

## 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.