



# NCSC-2026-0056

## Kwetsbaarheden verholpen in Microsoft Developer Tools

NCSC Advisory

Prioriteit: Normaal

Gepubliceerd op: 10-02-2026

**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 componenten van Visual Studio en .NET.

## Duiding

Een kwaadwillende kan de kwetsbaarheden misbruiken om beveiligingsmaatregelen te omzeilen, zich verhoogde rechten toe te kennen en mogelijk willekeurige code uit te voeren met rechten van het slachtoffer.

Voor succesvol misbruik moet de kwaadwillende het slachtoffer misleiden om malafide code te downloaden en uit te voeren. Omdat ontwikkelaars in ontwikkelomgevingen vaak met verhoogde rechten werken, is niet uit te sluiten dat de uitvoer van code ook plaatsvindt onder verhoogde rechten.

### GitHub Copilot and Visual Studio:

CVE-ID	CVSS	Impact
CVE-2026-21523	8.00	Uitvoeren van willekeurige code
CVE-2026-21257	8.00	Verkrijgen van verhoogde rechten
CVE-2026-21256	8.80	Uitvoeren van willekeurige code

### GitHub Copilot and Visual Studio Code:

CVE-ID	CVSS	Impact
CVE-2026-21518	6.50	Omzeilen van beveiligingsmaatregel

### .NET and Visual Studio:

CVE-ID	CVSS	Impact
CVE-2026-21218	7.50	Voordoen als andere gebruiker

### Github Copilot:

CVE-ID	CVSS	Impact
CVE-2026-21516	8.80	Uitvoeren van willekeurige code

|-----|-----|-----|

## 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-2026-21518	6.5 MEDIUM
> CVE-2026-21523	8.0 HIGH
> CVE-2026-21218	7.5 HIGH
> CVE-2026-21257	8.0 HIGH
> CVE-2026-21256	8.8 HIGH
> CVE-2026-21516	8.8 HIGH

## CWE's

CWE	Beschrijving
> CWE-77	Improper Neutralization of Special Elements used in a Command ('Command Injection')
> CWE-94	Improper Control of Generation of Code ('Code Injection')
> CWE-166	Improper Handling of Missing Special Element
> CWE-367	Time-of-check Time-of-use (TOCTOU) Race Condition

## Getroffen producten

Microsoft
.NET 10.0
.NET 10.0 installed on Linux
.NET 10.0 installed on Mac OS
.NET 10.0 installed on Windows
.NET 8.0
.NET 8.0 installed on Linux
.NET 8.0 installed on Mac OS
.NET 8.0 installed on Windows
.NET 9.0
.NET 9.0 installed on Linux
.NET 9.0 installed on Mac OS
.NET 9.0 installed on Windows
GitHub Copilot Plugin for JetBrains IDEs
Microsoft Visual Studio 2022 version 17.14

Microsoft Visual Studio 2022  
version 18.3

Visual Studio  
Code

## 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 or 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.