



NCSC-2026-0235

Kwetsbaarheden verholpen in Microsoft Developer Tools

NCSC Security Advisory

Prioriteit: Normaal

Gepubliceerd op: 14-07-2026

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).

Ontvangers van TLP:WHITE mogen de informatie publiek verspreiden.

Uw reacties zijn welkom op info@ncsc.nl

Feiten

Microsoft heeft kwetsbaarheden verholpen in Developer Tools als .NET en Visual Studio.

Duiding

Een kwaadwillende kan de kwetsbaarheden misbruiken om aanvallen uit te voeren die kunnen leiden tot schade uit de categorieën zoals genoemd in bijgevoegde tabel.

Voor succesvol misbruik moet de kwaadwillende het slachtoffer misleiden een malafide bronbestand te openen en verwerken in de ontwikkelomgeving.

Visual Studio:

CVE-ID	CVSS	Impact
CVE-2026-47305	7.80	Uitvoeren van willekeurige code

GitHub Copilot and Visual Studio Code:

CVE-ID	CVSS	Impact
CVE-2026-47282	6.50	Toegang tot gevoelige gegevens

Visual Studio Code:

CVE-ID	CVSS	Impact
CVE-2026-45496	5.50	Omzeilen van beveiligingsmaatregel
CVE-2026-50520	8.40	Uitvoeren van willekeurige code
CVE-2026-57101	7.10	Omzeilen van beveiligingsmaatregel
CVE-2026-57102	8.80	Omzeilen van beveiligingsmaatregel

.NET Framework:

CVE-ID	CVSS	Impact
CVE-2026-50524	7.50	Denial-of-Service

CVE-2026-50527	7.50	Denial-of-Service	
CVE-2026-50646	7.80	Uitvoeren van willekeurige code	
CVE-2026-50648	7.50	Denial-of-Service	
CVE-2026-50650	7.80	Uitvoeren van willekeurige code	
-----	-----	-----	

ASP.NET Core:

-----	-----	-----	
CVE-ID	CVSS	Impact	
-----	-----	-----	
CVE-2026-47300	8.80	Verkrijgen van verhoogde rechten	
CVE-2026-47303	8.80	Verkrijgen van verhoogde rechten	
CVE-2026-50506	7.50	Denial-of-Service	
CVE-2026-56170	7.50	Denial-of-Service	
CVE-2026-45646	7.50	Denial-of-Service	
-----	-----	-----	

.NET:

-----	-----	-----	
CVE-ID	CVSS	Impact	
-----	-----	-----	
CVE-2026-47302	7.50	Denial-of-Service	
CVE-2026-47304	8.10	Omzeilen van beveiligingsmaatregel	
CVE-2026-50525	7.50	Denial-of-Service	
CVE-2026-50526	7.00	Manipulatie van gegevens	
CVE-2026-50528	8.20	Omzeilen van beveiligingsmaatregel	
CVE-2026-50649	7.80	Uitvoeren van willekeurige code	
CVE-2026-50651	7.50	Denial-of-Service	
CVE-2026-50659	6.50	Voordoen als andere gebruiker	
-----	-----	-----	

.NET Core:

-----	-----	-----	
CVE-ID	CVSS	Impact	
-----	-----	-----	
CVE-2026-57108	7.50	Denial-of-Service	
-----	-----	-----	

GitHub Copilot and Visual Studio:

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

----- ----- -----
CVE-2026-41109 8.80 Omzeilen van beveiligingsmaatregel
----- ----- -----

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-2026-47300	8.8 HIGH
> CVE-2026-47302	7.5 HIGH
> CVE-2026-47303	8.8 HIGH
> CVE-2026-50524	7.5 HIGH
> CVE-2026-56170	7.5 HIGH
> CVE-2026-47304	8.1 HIGH
> CVE-2026-50525	7.5 HIGH
> CVE-2026-50526	7.0 HIGH
> CVE-2026-50527	7.5 HIGH
> CVE-2026-50528	8.2 HIGH
> CVE-2026-50648	7.5 HIGH
> CVE-2026-50651	7.5 HIGH
> CVE-2026-50659	6.5 MEDIUM

> CVE-2026-57108	7.5 HIGH
> CVE-2026-50646	7.8 HIGH
> CVE-2026-50649	7.8 HIGH
> CVE-2026-50650	7.8 HIGH
> CVE-2026-50506	7.5 HIGH
> CVE-2026-45646	7.5 HIGH
> CVE-2026-47282	6.5 MEDIUM
> CVE-2026-45496	5.5 MEDIUM
> CVE-2026-50520	8.4 HIGH
> CVE-2026-41109	8.8 HIGH
> CVE-2026-57101	7.1 HIGH
> CVE-2026-57102	8.8 HIGH
> CVE-2026-47305	7.8 HIGH

CWE's

CWE	Beschrijving
> CVE-200	Exposure of Sensitive Information to an Unauthorized Actor

Getroffen producten

Microsoft
.NET
.NET 10.0 installed on Linux
.NET 10.0 installed on Mac OS

.NET 10.0 installed on Windows
.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
.NET Framework
Azure
Microsoft Visual Studio 2022 version 17.14
Microsoft Visual Studio Code
Microsoft Visual Studio Code CoPilot Chat Extension
Microsoft.AspNetCore.OData
Microsoft.AspNetCore.OData
Visual Studio 2017
Visual Studio 2019
Visual Studio 2022

Visual Studio 2026
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 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.