



NCSC-2025-0079

Kwetsbaarheden verholpen in Microsoft Developer Tools

NCSC Advisory

Prioriteit: Normaal

Gepubliceerd op: 11-03-2025

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 Visual Studio en .NET

Duiding

Een kwadwillende kan de kwetsbaarheden misbruiken om zich verhoogde rechten toe te kennen en/of willekeurige code uit te voeren met rechten van de ontwikkelaar. Omdat ontwikkelaars veelal onder verhoogde rechten werken, is niet uit te sluiten dat uitvoer van code kan plaatsvinden met hogere rechten dan gebruikersrechten.

Voor succesvol misbruik van de kwetsbaarheden met kenmerken CVE-2025-24998, CVE-2025-25003 en CVE-2025-26631 moet de kwaadwillende het slachtoffer misleiden malafide broncode te importeren en uit te voeren. Voor succesvol misbruik van de kwetsbaarheden met kenmerken CVE-2025-24043 en CVE-2025-24070 moet de kwaadwillende voorafgaande authenticatie hebben en voorbereidende handelingen plegen. Misbruik is hiermee niet eenvoudig.

Visual Studio:

CVE-ID	CVSS	Impact
CVE-2025-24998	7.30	Verkrijgen van verhoogde rechten
CVE-2025-25003	7.30	Verkrijgen van verhoogde rechten

Visual Studio Code:

CVE-ID	CVSS	Impact
CVE-2025-26631	7.30	Verkrijgen van verhoogde rechten

.NET:

CVE-ID	CVSS	Impact
CVE-2025-24043	7.50	Uitvoeren van willekeurige code

ASP.NET Core & Visual Studio:

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

CVE-ID	CVSS	Impact
CVE-2025-24070	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
> CVE-2025-24043	7.7 HIGH
> CVE-2025-24070	
> CVE-2025-24998	
> CVE-2025-25003	
> CVE-2025-26631	

CWE's

CWE	Beschrijving
> CVE-1390	Weak Authentication
> CVE-347	Improper Verification of Cryptographic Signature
> CVE-427	Uncontrolled Search Path Element

Getroffen producten

Microsoft
ASP.NET Core 8.0
ASP.NET Core 9.0
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 Code
WinDbg

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.