



NCSC-2026-0143

Kwetsbaarheden verholpen in Microsoft Developer Tools

NCSC Advisory

Prioriteit: Normaal

Gepubliceerd op: 12-05-2026

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 diverse Developer Tools.

Duiding

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

- Denial-of-Service (DoS)
- Omzeilen van een beveiligingsmaatregel
- Uitvoeren van willekeurige code (gebruikersrechten)
- Toegang tot gevoelige gegevens

De kwetsbaarheid met kenmerk CVE-2026-42826 is centraal verholpen door Microsoft en slechts toegevoegd ter informatie. Er zijn hiervoor geen verdere acties benodigd.

Azure DevOps:

CVE-ID	CVSS	Impact
CVE-2026-42826	10.00	Toegang tot gevoelige gegevens

Visual Studio Code:

CVE-ID	CVSS	Impact
CVE-2026-41610	6.30	Omzeilen van beveiligingsmaatregel
CVE-2026-41611	7.80	Uitvoeren van willekeurige code
CVE-2026-41612	5.50	Toegang tot gevoelige gegevens
CVE-2026-41613	8.80	Verkrijgen van verhoogde rechten

Microsoft Data Formulator:

CVE-ID	CVSS	Impact
CVE-2026-41094	8.80	Uitvoeren van willekeurige code

ASP.NET Core:

CVE-ID	CVSS	Impact
CVE-2026-42899	7.50	Denial-of-Service

.NET:

CVE-ID	CVSS	Impact
CVE-2026-32177	7.30	Denial-of-Service
CVE-2026-35433	7.30	Verkrijgen van verhoogde rechten
CVE-2026-32175	4.30	<Vertaal: Tampering>

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-2026-32177	7.3 HIGH
> CVE-2026-35433	7.3 HIGH
> CVE-2026-32175	4.3 MEDIUM
> CVE-2026-42899	7.5 HIGH

> CVE-2026-41094	8.8 HIGH
> CVE-2026-41109	8.8 HIGH
> CVE-2026-41610	6.3 MEDIUM
> CVE-2026-41611	7.8 HIGH
> CVE-2026-41612	5.5 MEDIUM
> CVE-2026-41613	8.8 HIGH
> CVE-2026-42826	10.0 CRITICAL

CWE's

CWE	Beschrijving
> CWE-59	Improper Link Resolution Before File Access ('Link Following')
> CWE-74	Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')
> CWE-77	Improper Neutralization of Special Elements used in a Command ('Command Injection')
> CWE-78	Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')
> CWE-79	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')
> CWE-80	Improper Neutralization of Script-Related HTML Tags in a Web Page (Basic XSS)
> CWE-94	Improper Control of Generation of Code ('Code Injection')
> CWE-122	Heap-based Buffer Overflow
> CWE-190	Integer Overflow or Wraparound
> CWE-200	Exposure of Sensitive Information to an Unauthorized Actor
> CWE-384	Session Fixation
> CWE-835	Loop with Unreachable Exit Condition ('Infinite Loop')

➤ CWE-20	Improper Input Validation
➤ CWE-22	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')
➤ CWE-23	Relative Path Traversal
➤ CWE-36	Absolute Path Traversal

Getroffen producten

Microsoft
.NET 10.0 installed on Linux
.NET 10.0 installed on Mac OS
.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
Azure DevOps
Microsoft Data Formulator

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 17.12
Microsoft Visual Studio 2022 version 17.14
Microsoft Visual Studio 2026 version 18.5
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.