



NCSC-2026-0184

Kwetsbaarheden verholpen in Microsoft Developer Tools

NCSC Security Advisory

Prioriteit: Normaal

Gepubliceerd op: 09-06-2026

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.

Duiding

Een kwaadwillende kan de kwetsbaarheden misbruiken om aanvallen uit te voeren die kunnen leiden tot de categorieën schade, zoals beschreven in de onderstaande tabellen.

Met uitzondering van de kwetsbaarheid in .NET core, waarvoor geen voorafgaande authenticatie of gebruikersinteractie nodig is om een Denial-of-Service te veroorzaken, moet voor succesvol misbruik de kwaadwillende lokaal toegang hebben tot het kwetsbare systeem, of het slachtoffer misleiden een malafide broncodebestand te openen en uitvoeren.

Visual Studio Code:

| CVE-ID | CVSS | Impact |
|----------------|------|------------------------------------|
| CVE-2026-47287 | 6.50 | Manipulatie van gegevens |
| CVE-2026-47292 | 7.80 | Verkrijgen van verhoogde rechten |
| CVE-2026-40376 | 7.50 | Verkrijgen van verhoogde rechten |
| CVE-2026-47281 | 9.60 | Verkrijgen van verhoogde rechten |
| CVE-2026-47284 | 6.50 | Toegang tot gevoelige gegevens |
| CVE-2026-48569 | 7.10 | Omzeilen van beveiligingsmaatregel |

GitHub Copilot and Visual Studio Code:

| CVE-ID | CVSS | Impact |
|----------------|------|------------------------------------|
| CVE-2026-45482 | 8.40 | Omzeilen van beveiligingsmaatregel |

Microsoft Live Share Canvas SDK:

| CVE-ID | CVSS | Impact |
|----------------|------|----------------------------------|
| CVE-2026-45644 | 8.00 | Verkrijgen van verhoogde rechten |

ASP.NET Core:

| CVE-ID | CVSS | Impact |
|----------------|------|-------------------|
| CVE-2026-45591 | 7.50 | Denial-of-Service |

.NET:

| CVE-ID | CVSS | Impact |
|----------------|------|----------------------------------|
| CVE-2026-45490 | 7.80 | Verkrijgen van verhoogde rechten |
| CVE-2026-45491 | 6.20 | Manipulatie van gegevens |

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-2026-40376 | 7.5 HIGH |
| > CVE-2026-45482 | 8.4 HIGH |
| > CVE-2026-45490 | 7.8 HIGH |
| > CVE-2026-45491 | 6.2 MEDIUM |
| > CVE-2026-45591 | 7.5 HIGH |
| > CVE-2026-45644 | 8.0 HIGH |
| > CVE-2026-47281 | 9.6 CRITICAL |
| > CVE-2026-47284 | 6.5 MEDIUM |

| | |
|------------------|------------|
| > CVE-2026-47287 | 6.5 MEDIUM |
| > CVE-2026-47292 | 7.8 HIGH |
| > CVE-2026-48569 | 7.1 HIGH |

CWE's

| CWE | Beschrijving |
|-----------|--|
| > CWE-20 | Improper Input Validation |
| > CWE-22 | Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') |
| > CWE-23 | Relative Path Traversal |
| > CWE-59 | Improper Link Resolution Before File Access ('Link Following') |
| > CWE-79 | Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') |
| > CWE-94 | Improper Control of Generation of Code ('Code Injection') |
| > CWE-200 | Exposure of Sensitive Information to an Unauthorized Actor |
| > CWE-285 | Improper Authorization |
| > CWE-306 | Missing Authentication for Critical Function |
| > CWE-400 | Uncontrolled Resource Consumption |
| > CWE-522 | Insufficiently Protected Credentials |
| > CWE-798 | Use of Hard-coded Credentials |
| > CWE-829 | Inclusion of Functionality from Untrusted Control Sphere |
| > CWE-862 | Missing Authorization |

Getroffen producten

| Microsoft |
|------------------------------------|
| .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 installed on Linux |
| .NET 9.0 installed on Mac OS |
| .NET 9.0 installed on Windows |
| ASP.NET Core 10.0 |
| ASP.NET Core 8.0 |
| ASP.NET Core 9.0 |
| Microsoft Live Share Canvas SDK |

| |
|--|
| Microsoft Visual Studio 2026 version 18.6 |
| Microsoft Visual Studio Code CoPilot Chat Extension |
| Visual Studio Code |
| Visual Studio Code - MSSQL Extension |

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.