Nationaal Cyber Security Centrum
Ministerie van Justitie en Veiligheid

Advisory NCSC-2026-0473

PRIORITEIT: NORMAAL

Kwetsbaarheden verholpen in Microsoft Developer Tools

Publicatiedatum: 10-11-2026

Toegestane verspreiding: TLP:WHITE
(Traffic Light Protocol)

Deze publicatie bevat het label TLP:WHITE en wordt door het Nationaal Cyber Security Center (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 de-len. Dit staat beschreven in de standaard First (www.first.org/tlp).

Ontvangers van TLP:WHITE mogen de informatie publiek verspreiden.

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 categorieën schade zoals benoemd in onderstaande tabel.

De vereiste voorwaarden voor succesvol misbruik verschillen per kwetsbaarheid. Afhankelijk van de kwetsbaarheid kan misbruik gebruikersinteractie vereisen, zoals het openen of verwerken van een malafide bronbestand, of plaatsvinden via een kwetsbare applicatie of dienst.

Visual Studio Code - GitHub Pull Requests and Issues Extension:

CVE-ID	CVSS	Impact
CVE-2026-119976	6,50	Toegang tot gevoelige gegevens

Azure DevOps:

CVE-ID	CVSS	Impact
CVE-2026-109467	9,90	Uitvoeren van willekeurige code

Visual Studio Code:

CVE-ID	CVSS	Impact
CVE-2026-102230	7,40	Toegang tot gevoelige gegevens
CVE-2026-102236	8,60	Omzeilen van beveiligingsmaatregel
CVE-2026-114171	8,80	Omzeilen van beveiligingsmaatregel
CVE-2026-119975	8,80	Uitvoeren van willekeurige code
CVE-2026-119981	7,00	Verkrijgen van verhoogde rechten
CVE-2026-119982	6,50	Omzeilen van beveiligingsmaatregel
CVE-2026-119983	8,80	Omzeilen van beveiligingsmaatregel
CVE-2026-119985	8,30	Uitvoeren van willekeurige code
CVE-2026-120779	9,60	Uitvoeren van willekeurige code
CVE-2026-120780	8,30	Uitvoeren van willekeurige code
CVE-2026-120782	onb.	Omzeilen van beveiligingsmaatregel
CVE-2026-121660	7,50	Omzeilen van beveiligingsmaatregel
CVE-2026-121661	7,80	Omzeilen van beveiligingsmaatregel
CVE-2026-121662	8,60	Uitvoeren van willekeurige code
CVE-2026-121663	8,80	Omzeilen van beveiligingsmaatregel
CVE-2026-121664	8,30	Uitvoeren van willekeurige code
CVE-2026-121665	8,80	Omzeilen van beveiligingsmaatregel
CVE-2026-70094	8,80	Uitvoeren van willekeurige code

Visual Studio:

CVE-ID	CVSS	Impact
CVE-2026-114151	8,80	Uitvoeren van willekeurige code
CVE-2026-114152	8,80	Uitvoeren van willekeurige code
CVE-2026-114158	8,80	Uitvoeren van willekeurige code
CVE-2026-114159	8,80	Uitvoeren van willekeurige code
CVE-2026-118745	8,80	Uitvoeren van willekeurige code

.NET Aspire:

CVE-ID	CVSS	Impact
CVE-2026-120778	7,30	Verkrijgen van verhoogde rechten

ASP.NET Core:

CVE-ID	CVSS	Impact
CVE-2026-109476	6,10	Toegang tot gevoelige gegevens
CVE-2026-109478	7,50	Denial-of-Service
CVE-2026-109481	7,50	Verkrijgen van verhoogde rechten
CVE-2026-114146	9,00	Verkrijgen van verhoogde rechten
CVE-2026-114147	7,50	Denial-of-Service
CVE-2026-114149	7,50	Denial-of-Service
CVE-2026-114150	5,90	Toegang tot gevoelige gegevens
CVE-2026-114154	7,50	Denial-of-Service
CVE-2026-114156	6,50	Omzeilen van beveiligingsmaatregel
CVE-2026-114157	7,50	Omzeilen van beveiligingsmaatregel
CVE-2026-118748	7,50	Denial-of-Service
CVE-2026-118749	7,50	Denial-of-Service
CVE-2026-118750	7,50	Denial-of-Service
CVE-2026-114153	4,00	Omzeilen van beveiligingsmaatregel

.NET:

CVE-ID	CVSS	Impact
CVE-2026-105544	7,50	Verkrijgen van verhoogde rechten
CVE-2026-109475	7,50	Denial-of-Service
CVE-2026-114155	7,50	Verkrijgen van verhoogde rechten
CVE-2026-118746	6,80	Omzeilen van beveiligingsmaatregel

Azure DevOps Server:

CVE-ID	CVSS	Impact
CVE-2026-112745	6,50	Toegang tot gevoelige gegevens
CVE-2026-85923	8,80	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

Referenties

- https://portal.msrc.microsoft.com/en-us/security-guidance

Kwetsbaarheden

CVE	CVSS Score
CVE-2026-70094	8.8 HIGH
CVE-2026-70175	8.1 HIGH
CVE-2026-85923	8.8 HIGH
CVE-2026-102230	7.4 HIGH
CVE-2026-102236	8.6 HIGH
CVE-2026-105544	7.5 HIGH
CVE-2026-109467	9.9 CRITICAL
CVE-2026-109475	7.5 HIGH
CVE-2026-109476	6.1 MEDIUM
CVE-2026-109478	7.5 HIGH
CVE-2026-109481	7.5 HIGH
CVE-2026-112745	6.5 MEDIUM
CVE-2026-114146	9.0 CRITICAL
CVE-2026-114147	7.5 HIGH
CVE-2026-114149	7.5 HIGH
CVE-2026-114150	5.9 MEDIUM
CVE-2026-114151	8.8 HIGH

CVE	CVSS Score
CVE-2026-114152	8.8 HIGH
CVE-2026-114154	7.5 HIGH
CVE-2026-114155	7.5 HIGH
CVE-2026-114156	6.5 MEDIUM
CVE-2026-114157	7.5 HIGH
CVE-2026-114158	8.8 HIGH
CVE-2026-114159	8.8 HIGH
CVE-2026-114171	8.8 HIGH
CVE-2026-118741	8.1 HIGH
CVE-2026-118745	8.8 HIGH
CVE-2026-118746	6.8 MEDIUM
CVE-2026-118747	7.5 HIGH
CVE-2026-118748	7.5 HIGH
CVE-2026-118749	7.5 HIGH
CVE-2026-118750	7.5 HIGH
CVE-2026-119975	8.8 HIGH
CVE-2026-119976	6.5 MEDIUM
CVE-2026-119981	7.0 HIGH
CVE-2026-119982	6.5 MEDIUM
CVE-2026-119983	8.8 HIGH
CVE-2026-119985	8.3 HIGH
CVE-2026-120778	7.3 HIGH
CVE-2026-120779	9.6 CRITICAL
CVE-2026-120780	8.3 HIGH
CVE-2026-120782	7.8 HIGH
CVE-2026-120796	5.3 MEDIUM
CVE-2026-121660	7.5 HIGH
CVE-2026-121661	7.8 HIGH
CVE-2026-121662	8.6 HIGH
CVE-2026-121663	8.8 HIGH
CVE-2026-121664	8.3 HIGH

CVE	CVSS Score
CVE-2026-121665	8.8 HIGH

CWE's

CWE	Beschrijving
CWE-73	External Control of File Name or Path
CWE-77	Improper Neutralization of Special Elements used in a Command
CWE-79	Improper Neutralization of Input During Web Page Generation
CWE-94	Improper Control of Generation of Code
CWE-116	Improper Encoding or Escaping of Output
CWE-121	Stack-based Buffer Overflow
CWE-122	Heap-based Buffer Overflow
CWE-184	Incomplete List of Disallowed Inputs
CWE-306	Missing Authentication for Critical Functionality
CWE-352	Cross-Site Request Forgery
CWE-362	Concurrent Execution using Shared Resource with Improper Synchronization
CWE-367	Time-of-check Time-of-use (TOCTOU) Race Condition
CWE-379	Creation of Temporary File in Directory with Insecure Permissions
CWE-401	Missing Release of Memory after Effective Lifetime
CWE-407	Inefficient Algorithmic Complexity
CWE-426	Untrusted Search Path
CWE-436	Interpretation Conflict
CWE-451	User Interface (UI) Misrepresentation of Critical Information
CWE-501	Trust Boundary Violation
CWE-502	Deserialization of Untrusted Data
CWE-636	Not Failing Securely
CWE-639	Authorization Bypass Through User-Controlled Key
CWE-770	Allocation of Resources Without Limits or Throttling
CWE-822	Untrusted Pointer Dereference

CWE	Beschrijving
CWE-862	Missing Authorization
CWE-863	Incorrect Authorization
CWE-908	Use of Uninitialized Resource
CWE-918	Server-Side Request Forgery
CWE-1021	Improper Restriction of Rendered UI Layers or Frames

Getroffen producten

Microsoft
.NET 10.0 installed on Linux
.NET 10.0 installed on Mac OS
.NET 10.0 installed on Windows
.NET 11.0 installed on Linux
.NET 11.0 installed on Mac OS
.NET 11.0 installed on Windows
.NET 6.0
.NET 6.0 installed on Linux
.NET 6.0 installed on Mac OS
.NET 6.0 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 Aspire 13.5.4 for Linux
.NET Aspire 13.5.4 for macOS
ASP.NET Core 10.0
ASP.NET Core 2.3

Microsoft
ASP.NET Core 8.0
Aspire.Cli on Linux
Aspire.Cli on Mac OS
Azure DevOps
Azure DevOps Server
Azure DevOps Server 2025
Microsoft Visual Studio 2022 version 17.14
Microsoft Visual Studio 2026 version 18.11
Microsoft Visual Studio 2026 version 18.12
Microsoft Visual Studio 2026 version 18.13
Microsoft.AspNetCore.Http
Microsoft.AspNetCore.SignalR.StackExchangeRedis on .NET 10.0 installed on Linux
Microsoft.AspNetCore.SignalR.StackExchangeRedis on .NET 10.0 installed on Mac OS
Microsoft.AspNetCore.SignalR.StackExchangeRedis on .NET 10.0 installed on Windows
Microsoft.AspNetCore.SignalR.StackExchangeRedis on .NET 11.0 installed on Linux
Microsoft.AspNetCore.SignalR.StackExchangeRedis on .NET 11.0 installed on Mac OS
Microsoft.AspNetCore.SignalR.StackExchangeRedis on .NET 11.0 installed on Windows
Microsoft.AspNetCore.SignalR.StackExchangeRedis on .NET 6.0 installed on Linux
Microsoft.AspNetCore.SignalR.StackExchangeRedis on .NET 6.0 installed on Mac OS
Microsoft.AspNetCore.SignalR.StackExchangeRedis on .NET 6.0 installed on Windows
Microsoft.AspNetCore.SignalR.StackExchangeRedis on .NET 8.0 installed on Linux
Microsoft.AspNetCore.SignalR.StackExchangeRedis on .NET 8.0 installed on Mac OS
Microsoft.AspNetCore.SignalR.StackExchangeRedis on .NET 8.0 installed on Windows
Microsoft.AspNetCore.SignalR.StackExchangeRedis on .NET 9.0 installed on Linux
Microsoft.AspNetCore.SignalR.StackExchangeRedis on .NET 9.0 installed on Mac OS
Microsoft.AspNetCore.SignalR.StackExchangeRedis on .NET 9.0 installed on Windows
Microsoft.AspNetCore.WebUtilities
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.