



Advisory NCSC-2026-0426

PRIORITEIT: NORMAAL

Kwetsbaarheden verholpen in Microsoft Developer Tools

Publicatiedatum: 13-10-2026

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 delen. 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 componenten van de Developer Tools, zoals .NET en Visual Studio.

Duiding

Een kwaadwillende kan aanvallen uitvoeren die kunnen leiden tot de categorieën schade zoals weergegeven in de onderstaande tabellen.

.NET: ----- ----- -----		
CVE-ID	CVSS	Impact
CVE-2026-58280	7.50	Denial-of-Service
CVE-2026-66822	5.90	Toegang tot gevoelige gegevens
CVE-2026-69651	7.50	Denial-of-Service
CVE-2026-70161	7.30	Verkrijgen van verhoogde rechten
CVE-2026-70165	6.70	Verkrijgen van verhoogde rechten
CVE-2026-70174	8.80	Uitvoeren van willekeurige code
CVE-2026-70190	7.30	Verkrijgen van verhoogde rechten
CVE-2026-70197	8.10	Uitvoeren van willekeurige code
CVE-2026-83520	8.80	Uitvoeren van willekeurige code
CVE-2026-84008	7.50	Denial-of-Service
CVE-2026-87697	8.80	Uitvoeren van willekeurige code, <Vertaal: >
CVE-2026-96224	8.80	Uitvoeren van willekeurige code
CVE-2026-96225	7.80	Verkrijgen van verhoogde rechten
CVE-2026-96229	6.50	Toegang tot gevoelige gegevens
CVE-2026-96231	7.80	Verkrijgen van verhoogde rechten
CVE-2026-96232	7.50	Toegang tot gevoelige gegevens
CVE-2026-96234	5.30	Toegang tot gevoelige gegevens
CVE-2026-96235	8.80	Uitvoeren van willekeurige code
CVE-2026-96237	7.50	Uitvoeren van willekeurige code
CVE-2026-96238	6.50	Omzeilen van beveiligingsmaatregel
CVE-2026-96957	8.80	Omzeilen van beveiligingsmaatregel
CVE-2026-96958	7.50	Denial-of-Service
CVE-2026-96959	7.50	Denial-of-Service
CVE-2026-96960	7.50	Denial-of-Service
-----	---	-----

Visual Studio Code: |-----|-----|-----|

CVE-ID	CVSS	Impact
CVE-2026-102229	6.80	Toegang tot gevoelige gegevens
CVE-2026-102230	7.40	Toegang tot gevoelige gegevens
CVE-2026-102231	7.70	Omzeilen van beveiligingsmaatregel
CVE-2026-102232	7.00	Omzeilen van beveiligingsmaatregel
CVE-2026-102233	7.80	Omzeilen van beveiligingsmaatregel
CVE-2026-102234	7.40	Omzeilen van beveiligingsmaatregel
CVE-2026-102235	8.80	Uitvoeren van willekeurige code
CVE-2026-102238	9.60	Uitvoeren van willekeurige code
CVE-2026-102851	6.10	Omzeilen van beveiligingsmaatregel
CVE-2026-69370	8.80	Uitvoeren van willekeurige code
CVE-2026-70098	8.80	Uitvoeren van willekeurige code

ASP.NET Core: |-----|-----|-----|

CVE-ID	CVSS	Impact
CVE-2026-102870	8.80	Uitvoeren van willekeurige code
CVE-2026-70159	7.50	Denial-of-Service
CVE-2026-70175	8.10	Verkrijgen van verhoogde rechten
CVE-2026-70179	7.50	Verkrijgen van verhoogde rechten
CVE-2026-70181	7.50	Denial-of-Service
CVE-2026-70183	7.50	Verkrijgen van verhoogde rechten
CVE-2026-70186	7.50	Denial-of-Service
CVE-2026-70188	9.10	Omzeilen van beveiligingsmaatregel
CVE-2026-70196	5.90	Denial-of-Service
CVE-2026-88092	9.40	<Vertaal: Tampering>
CVE-2026-96230	8.80	Uitvoeren van willekeurige code
CVE-2026-96233	7.50	Denial-of-Service
CVE-2026-96236	7.50	Denial-of-Service

Visual Studio Tools for Applications and SQL Server Management Studio:

CVE-ID	CVSS	Impact
CVE-2026-103572	8.80	Uitvoeren van willekeurige code

Windows AppX Deployment Extensions: |-----|-----|-----|

CVE-ID	CVSS	Impact
CVE-2026-69945	8.80	Verkrijgen van verhoogde rechten

.NET Framework: |-----|-----|-----|

CVE-ID	CVSS	Impact
CVE-2026-108398	8.80	Omzeilen van beveiligingsmaatregel
CVE-2026-70007	8.80	Uitvoeren van willekeurige code
CVE-2026-70035	8.80	Uitvoeren van willekeurige code
CVE-2026-70194	6.50	Omzeilen van beveiligingsmaatregel
CVE-2026-85363	8.80	Verkrijgen van verhoogde rechten

Windows AppX Deployment Service: |-----|-----|-----|

CVE-ID	CVSS	Impact
CVE-2026-69905	5.50	<Vertaal: Tampering>
CVE-2026-69914	5.50	Toegang tot gevoelige gegevens
CVE-2026-69969	4.70	Toegang tot gevoelige gegevens
CVE-2026-69979	5.50	Omzeilen van beveiligingsmaatregel
CVE-2026-85849	7.80	Verkrijgen van verhoogde rechten
CVE-2026-85934	7.00	Verkrijgen van verhoogde rechten

.NET and Visual Studio: |-----|-----|-----|

CVE-ID	CVSS	Impact
CVE-2026-102869	8.80	Verkrijgen van verhoogde rechten, <Vertaal: >

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-2026-58280	
CVE-2026-66822	
CVE-2026-69370	
CVE-2026-69651	
CVE-2026-69905	
CVE-2026-69914	
CVE-2026-69945	
CVE-2026-69969	
CVE-2026-69979	
CVE-2026-70007	
CVE-2026-70035	

CVE	CVSS Score
CVE-2026-70098	
CVE-2026-70159	
CVE-2026-70161	
CVE-2026-70165	
CVE-2026-70174	
CVE-2026-70175	
CVE-2026-70179	
CVE-2026-70181	
CVE-2026-70183	
CVE-2026-70186	
CVE-2026-70188	
CVE-2026-70190	
CVE-2026-70194	
CVE-2026-70196	
CVE-2026-70197	
CVE-2026-83520	
CVE-2026-84008	
CVE-2026-85363	
CVE-2026-85849	
CVE-2026-85934	
CVE-2026-87697	
CVE-2026-88092	
CVE-2026-96224	
CVE-2026-96225	
CVE-2026-96229	
CVE-2026-96230	
CVE-2026-96231	
CVE-2026-96232	
CVE-2026-96233	
CVE-2026-96234	
CVE-2026-96235	
CVE-2026-96236	

CVE	CVSS Score
CVE-2026-96237	
CVE-2026-96238	
CVE-2026-96957	
CVE-2026-96958	
CVE-2026-96959	
CVE-2026-96960	
CVE-2026-102229	
CVE-2026-102230	
CVE-2026-102231	
CVE-2026-102232	
CVE-2026-102233	
CVE-2026-102234	
CVE-2026-102235	
CVE-2026-102238	
CVE-2026-102851	
CVE-2026-102870	
CVE-2026-103572	
CVE-2026-108398	
CVE-2026-102869	

CWE's

CWE	Beschrijving
CWE-22	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')
CWE-41	Improper Resolution of Path Equivalence
CWE-59	Improper Link Resolution Before File Access ('Link Following')
CWE-77	Improper Neutralization of Special Elements used in a Command ('Command Injection')
CWE-79	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')

CWE	Beschrijving
CWE-94	Improper Control of Generation of Code ('Code Injection')
CWE-116	Improper Encoding or Escaping of Output
CWE-125	Out-of-bounds Read
CWE-183	Permissive List of Allowed Inputs
CWE-190	Integer Overflow or Wraparound
CWE-201	Insertion of Sensitive Information Into Sent Data
CWE-266	Incorrect Privilege Assignment
CWE-290	Authentication Bypass by Spoofing
CWE-295	Improper Certificate Validation
CWE-346	Origin Validation Error
CWE-347	Improper Verification of Cryptographic Signature
CWE-358	Improperly Implemented Security Check for Standard
CWE-362	Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')
CWE-405	Asymmetric Resource Consumption (Amplification)
CWE-407	Inefficient Algorithmic Complexity
CWE-416	Use After Free
CWE-424	Improper Protection of Alternate Path
CWE-426	Untrusted Search Path
CWE-444	Inconsistent Interpretation of HTTP Requests ('HTTP Request/Response Smuggling')
CWE-502	Deserialization of Untrusted Data
CWE-674	Uncontrolled Recursion
CWE-770	Allocation of Resources Without Limits or Throttling
CWE-787	Out-of-bounds Write
CWE-807	Reliance on Untrusted Inputs in a Security Decision
CWE-829	Inclusion of Functionality from Untrusted Control Sphere
CWE-833	Deadlock
CWE-843	Access of Resource Using Incompatible Type ('Type Confusion')
CWE-862	Missing Authorization
CWE-863	Incorrect Authorization

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 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 11.0
ASP.NET Core 8.0
ASP.NET Core 9.0
Azure API Center
Microsoft .NET Framework 3.5 AND 4.8.1 on Windows 11 version 26H2
Microsoft .NET Framework 3.5 AND 4.8.1 on Windows Server 2022
Microsoft .NET Framework 3.5 AND 4.8.1 on Windows Server 2025
Microsoft .NET Framework 4.8
Microsoft .NET Framework 4.8.1 on Windows 11 version 26H1
Microsoft Visual Studio 2022 version 17.14
Microsoft.AspNetCore.Components.WebAssembly.Server on .NET 8.0 installed on Linux
Microsoft.AspNetCore.Components.WebAssembly.Server on .NET 8.0 installed on Mac OS
Microsoft.AspNetCore.Components.WebAssembly.Server on .NET 8.0 installed on Windows
System.Security.Cryptography.Xml on .NET 10.0 installed on Linux
System.Security.Cryptography.Xml on .NET 10.0 installed on Mac OS
System.Security.Cryptography.Xml on .NET 10.0 installed on Windows

Microsoft

`System.Security.Cryptography.Xml` on .NET 11.0 installed on Linux

`System.Security.Cryptography.Xml` on .NET 11.0 installed on Mac OS

`System.Security.Cryptography.Xml` on .NET 11.0 installed on Windows

`System.Security.Cryptography.Xml` on .NET 9.0 installed on Linux

`System.Security.Cryptography.Xml` on .NET 9.0 installed on Mac OS

`System.Security.Cryptography.Xml` on .NET 9.0 installed on Windows

`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 or 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.