



NCSC-2026-0285

Kwetsbaarheden verholpen in Microsoft Developer Tools

NCSC Security Advisory

Prioriteit: Normaal

Gepubliceerd op: 11-08-2026

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 categorieën schade zoals benoemd in onderstaande tabel.

Voor succesvol misbruik moet de kwaadwillende het slachtoffer misleiden een malafide broncodebestand te importeren en verwerken.

Visual Studio Code CoPilot Chat Extension:

CVE-ID	CVSS	Impact
CVE-2026-65675	7.10	Omzeilen van beveiligingsmaatregel

Microsoft PowerShell Core:

CVE-ID	CVSS	Impact
CVE-2026-58612	7.40	Toegang tot gevoelige gegevens
CVE-2026-70337	8.80	Uitvoeren van willekeurige code

GitHub Copilot and Visual Studio Code:

CVE-ID	CVSS	Impact
CVE-2026-70335	7.80	Verkrijgen van verhoogde rechten

Visual Studio Code:

CVE-ID	CVSS	Impact
CVE-2026-58650	7.80	Omzeilen van beveiligingsmaatregel
CVE-2026-59113	8.80	Uitvoeren van willekeurige code
CVE-2026-47285	6.50	Toegang tot gevoelige gegevens

CVE-2026-69320	8.80	Uitvoeren van willekeurige code	
CVE-2026-69278	7.80	Omzeilen van beveiligingsmaatregel	
CVE-2026-69306	8.20	Omzeilen van beveiligingsmaatregel	
CVE-2026-70336	8.80	Uitvoeren van willekeurige code	
-----	-----	-----	

.NET Framework:

-----	-----	-----	
CVE-ID	CVSS	Impact	
-----	-----	-----	
CVE-2026-62897	7.00	Uitvoeren van willekeurige code	
CVE-2026-62872	8.80	Verkrijgen van verhoogde rechten	
CVE-2026-65810	7.80	Verkrijgen van verhoogde rechten	
-----	-----	-----	

Microsoft PowerShell:

-----	-----	-----	
CVE-ID	CVSS	Impact	
-----	-----	-----	
CVE-2026-59119	7.30	Verkrijgen van verhoogde rechten	
CVE-2026-70338	7.80	Omzeilen van beveiligingsmaatregel	
-----	-----	-----	

.NET:

-----	-----	-----	
CVE-ID	CVSS	Impact	
-----	-----	-----	
CVE-2026-62899	5.90	Omzeilen van beveiligingsmaatregel	
CVE-2026-62900	5.90	Toegang tot gevoelige gegevens	
CVE-2026-62901	7.50	Denial-of-Service	
CVE-2026-62902	6.50	Toegang tot gevoelige gegevens	
CVE-2026-62909	7.80	Verkrijgen van verhoogde rechten	
CVE-2026-58641	7.80	Verkrijgen van verhoogde rechten	
CVE-2026-62871	7.80	Uitvoeren van willekeurige code	
CVE-2026-62886	7.80	Verkrijgen van verhoogde rechten	
CVE-2026-70354	7.80	Uitvoeren van willekeurige code	
-----	-----	-----	

Visual Studio Code - Python extension:

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

----- ----- -----
CVE-2026-54981 7.80 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-2026-58612	7.4 HIGH
> CVE-2026-59119	7.3 HIGH
> CVE-2026-70338	7.8 HIGH
> CVE-2026-70337	8.8 HIGH
> CVE-2026-58650	7.8 HIGH
> CVE-2026-59113	8.8 HIGH
> CVE-2026-47285	6.5 MEDIUM
> CVE-2026-69320	8.8 HIGH
> CVE-2026-69278	7.8 HIGH
> CVE-2026-69306	8.2 HIGH
> CVE-2026-70335	7.8 HIGH
> CVE-2026-70336	8.8 HIGH
> CVE-2026-62897	7.0 HIGH

> CVE-2026-62872	8.8 HIGH
> CVE-2026-65810	7.8 HIGH
> CVE-2026-62899	5.9 MEDIUM
> CVE-2026-62900	5.9 MEDIUM
> CVE-2026-62901	7.5 HIGH
> CVE-2026-62902	6.5 MEDIUM
> CVE-2026-62909	7.8 HIGH
> CVE-2026-58641	7.8 HIGH
> CVE-2026-62871	7.8 HIGH
> CVE-2026-62886	7.8 HIGH
> CVE-2026-70354	7.8 HIGH
> CVE-2026-65675	7.1 HIGH
> CVE-2026-54981	7.8 HIGH

CWE's

CWE	Beschrijving
> CWE-20	Improper Input Validation
> CWE-23	Relative Path Traversal
> 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-94	Improper Control of Generation of Code ('Code Injection')
> CWE-122	Heap-based Buffer Overflow
> CWE-190	Integer Overflow or Wraparound

> CWE-212	Improper Removal of Sensitive Information Before Storage or Transfer
> CWE-248	Uncaught Exception
> CWE-276	Incorrect Default Permissions
> CWE-444	Inconsistent Interpretation of HTTP Requests ('HTTP Request/Response Smuggling')
> CWE-606	Unchecked Input for Loop Condition
> CWE-636	Not Failing Securely ('Failing Open')
> CWE-639	Authorization Bypass Through User-Controlled Key
> CWE-693	Protection Mechanism Failure
> CWE-787	Out-of-bounds Write
> CWE-829	Inclusion of Functionality from Untrusted Control Sphere
> CWE-862	Missing Authorization
> CWE-863	Incorrect Authorization
> CWE-918	Server-Side Request Forgery (SSRF)

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 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
Microsoft .NET Framework 3.5 AND 4.6.2/4.7/4.7.1/4.7.2 on Windows 10 Version 1607 for 32-bit Systems
Microsoft .NET Framework 3.5 AND 4.6.2/4.7/4.7.1/4.7.2 on Windows 10 Version 1607 for x64-based Systems
Microsoft .NET Framework 3.5 AND 4.6.2/4.7/4.7.1/4.7.2 on Windows Server 2016
Microsoft .NET Framework 3.5 AND 4.6.2/4.7/4.7.1/4.7.2 on Windows Server 2016 (Server Core installation)
Microsoft .NET Framework 3.5 AND 4.7.2 on Windows 10 Version 1809 for 32-bit Systems
Microsoft .NET Framework 3.5 AND 4.7.2 on Windows 10 Version 1809 for ARM64-based Systems
Microsoft .NET Framework 3.5 AND 4.7.2 on Windows 10 Version 1809 for x64-based Systems
Microsoft .NET Framework 3.5 AND 4.7.2 on Windows Server 2019
Microsoft .NET Framework 3.5 AND 4.7.2 on Windows Server 2019 (Server Core installation)
Microsoft .NET Framework 3.5 AND 4.8 on Windows 10 Version 1809 for 32-bit Systems
Microsoft .NET Framework 3.5 AND 4.8 on Windows 10 Version 1809 for ARM64-based Systems
Microsoft .NET Framework 3.5 AND 4.8 on Windows 10 Version 1809 for x64-based Systems

Microsoft .NET Framework 3.5 AND 4.8 on
Windows 10 Version 21H2 for 32-bit Systems

Microsoft .NET Framework 3.5 AND 4.8 on Windows
10 Version 21H2 for ARM64-based Systems

Microsoft .NET Framework 3.5 AND 4.8 on Windows
10 Version 21H2 for x64-based Systems

Microsoft .NET Framework 3.5 AND 4.8 on
Windows 10 Version 22H2 for 32-bit Systems

Microsoft .NET Framework 3.5 AND 4.8 on Windows
10 Version 22H2 for ARM64-based Systems

Microsoft .NET Framework 3.5 AND 4.8 on Windows
10 Version 22H2 for x64-based Systems

Microsoft .NET Framework 3.5 AND 4.8
on Windows Server 2019

Microsoft .NET Framework 3.5 AND 4.8 on
Windows Server 2019 (Server Core installation)

Microsoft .NET Framework 3.5 AND 4.8
on Windows Server 2022

Microsoft .NET Framework 3.5 AND 4.8 on
Windows Server 2022 (Server Core installation)

Microsoft .NET Framework 3.5 AND 4.8.1 on
Windows 10 Version 21H2 for 32-bit Systems

Microsoft .NET Framework 3.5 AND 4.8.1 on Windows
10 Version 21H2 for ARM64-based Systems

Microsoft .NET Framework 3.5 AND 4.8.1 on
Windows 10 Version 21H2 for x64-based Systems

Microsoft .NET Framework 3.5 AND 4.8.1 on
Windows 10 Version 22H2 for 32-bit Systems

Microsoft .NET Framework 3.5 AND 4.8.1 on Windows
10 Version 22H2 for ARM64-based Systems

Microsoft .NET Framework 3.5 AND 4.8.1 on
Windows 10 Version 22H2 for x64-based Systems

Microsoft .NET Framework 3.5 AND 4.8.1 on Windows 11 Version 23H2 for ARM64-based Systems
Microsoft .NET Framework 3.5 AND 4.8.1 on Windows 11 Version 23H2 for x64-based Systems
Microsoft .NET Framework 3.5 AND 4.8.1 on Windows 11 Version 24H2 for ARM64-based Systems
Microsoft .NET Framework 3.5 AND 4.8.1 on Windows 11 Version 24H2 for x64-based Systems
Microsoft .NET Framework 3.5 AND 4.8.1 on Windows 11 Version 25H2 for ARM64-based Systems
Microsoft .NET Framework 3.5 AND 4.8.1 on Windows 11 Version 25H2 for x64-based Systems
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 2022 (Server Core installation)
Microsoft .NET Framework 3.5 AND 4.8.1 on Windows Server 2025
Microsoft .NET Framework 3.5 AND 4.8.1 on Windows Server 2025 (Server Core installation)
Microsoft .NET Framework 3.5 on Windows 11 Version 26H1 for ARM64-based Systems
Microsoft .NET Framework 3.5 on Windows 11 version 26H1 for x64-based Systems
Microsoft .NET Framework 3.5 on Windows Server 2012
Microsoft .NET Framework 3.5 on Windows Server 2012 (Server Core installation)
Microsoft .NET Framework 3.5 on Windows Server 2012 R2
Microsoft .NET Framework 3.5 on Windows Server 2012 R2 (Server Core installation)

Microsoft .NET Framework
4.6.2/4.7/4.7.1/4.7.2 on Windows Server
2012

Microsoft .NET Framework 4.6.2/4.7/4.7.1/4.7.2 on
Windows Server 2012 (Server Core installation)

Microsoft .NET Framework
4.6.2/4.7/4.7.1/4.7.2 on Windows Server 2012
R2

Microsoft .NET Framework 4.6.2/4.7/4.7.1/4.7.2 on
Windows Server 2012 R2 (Server Core installation)

Microsoft .NET Framework 4.8 on Windows 10
Version 1607 for 32-bit Systems

Microsoft .NET Framework 4.8 on Windows 10
Version 1607 for x64-based Systems

Microsoft .NET Framework 4.8 on
Windows Server 2012

Microsoft .NET Framework 4.8 on Windows
Server 2012 (Server Core installation)

Microsoft .NET Framework 4.8 on
Windows Server 2012 R2

Microsoft .NET Framework 4.8 on Windows
Server 2012 R2 (Server Core installation)

Microsoft .NET Framework 4.8 on
Windows Server 2016

Microsoft .NET Framework 4.8 on Windows
Server 2016 (Server Core installation)

Microsoft .NET Framework 4.8.1 on Windows 11
Version 26H1 for ARM64-based Systems

Microsoft .NET Framework 4.8.1 on Windows 11
version 26H1 for x64-based Systems

Microsoft Visual Studio 2022
version 17.14

Microsoft Visual Studio 2026 version 18.8
Microsoft Visual Studio Code CoPilot Chat Extension
PowerShell 7.4
PowerShell 7.5
PowerShell 7.6
Python extension for Visual Studio Code
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.