Nationaal Cyber Security Centrum
Ministerie van Justitie en Veiligheid

NCSC-2026-0351

Kwetsbaarheden verholpen in Microsoft Developer Tools

NCSC Security Advisory
Prioriteit: Normaal
Gepubliceerd op: 08-09-2026

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 15 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 ernstigste kwetsbaarheid met kenmerk CVE-2026-81376 heeft een CVSS-score van 9,6. Een kwaadwillende misbruiken door een gebruiker ertoe te verleiden een speciaal geprepareerde Visual Studio Code-workspace te openen. Hiermee kunnen de Workspace Trust-beperkingen worden omzeild, waardoor inhoud uit een niet-vertrouwde workspace opdrachten of code kan uitvoeren zonder dat de gebruiker hiervoor eerst toestemming geeft. Hierdoor kan de kwaadwillende toegang krijgen tot lokale gegevens of code uitvoeren met de rechten van de gebruiker.

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

.NET:

CVE-ID	CVSS	Impact
CVE-2026-58649	6,50	Toegang tot gevoelige gegevens

GitHub Copilot and Visual Studio Code:

CVE-ID	CVSS	Impact
CVE-2026-81380	5,30	Toegang tot gevoelige gegevens
CVE-2026-81381	6,50	Toegang tot gevoelige gegevens

Visual Studio Code:

CVE-ID	CVSS	Impact
CVE-2026-70334	7,80	Omzeilen van beveiligingsmaatregel
CVE-2026-78461	7,40	Omzeilen van beveiligingsmaatregel
CVE-2026-78462	8,80	Omzeilen van beveiligingsmaatregel
CVE-2026-81356	8,20	Omzeilen van beveiligingsmaatregel

CVE-2026-81357	8,20	Omzeilen van beveiligingsmaatregel
CVE-2026-81376	9,60	Omzeilen van beveiligingsmaatregel
CVE-2026-81377	6,50	<Vertaal: Tampering>
CVE-2026-81378	8,20	Omzeilen van beveiligingsmaatregel
CVE-2026-81379	8,20	Omzeilen van beveiligingsmaatregel
CVE-2026-81383	7,40	Toegang tot gevoelige gegevens

ASP.NET Core:

CVE-ID	CVSS	Impact
CVE-2026-57099	7,50	Denial-of-Service
CVE-2026-69304	5,90	Denial-of-Service

---------- Productgroep Apps ----------

All CVE's for this product group:
CVE-2026-58611, CVE-2026-80097

Microsoft Authenticator:

CVE-ID	CVSS	Impact
CVE-2026-80097	8,60	Verkrijgen van verhoogde rechten

XBox Gaming Services:

CVE-ID	CVSS	Impact
CVE-2026-58611	7,80	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-2026-57099	
CVE-2026-58649	
CVE-2026-69304	
CVE-2026-70334	
CVE-2026-78461	
CVE-2026-78462	
CVE-2026-81356	
CVE-2026-81357	
CVE-2026-81376	
CVE-2026-81377	
CVE-2026-81378	
CVE-2026-81379	
CVE-2026-81380	
CVE-2026-81381	

- CVE-2026-81383

CWE's

CWE	Beschrijving
CWE-22	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')
CWE-77	Improper Neutralization of Special Elements used in a Command ('Command Injection')
CWE-184	Incomplete List of Disallowed Inputs
CWE-346	Origin Validation Error
CWE-409	Improper Handling of Highly Compressed Data (Data Amplification)
CWE-436	Interpretation Conflict
CWE-444	Inconsistent Interpretation of HTTP Requests ('HTTP Request/Response Smuggling')
CWE-522	Insufficiently Protected Credentials
CWE-636	Not Failing Securely ('Failing Open')
CWE-639	Authorization Bypass Through User-Controlled Key
CWE-706	Use of Incorrectly-Resolved Name or Reference
CWE-770	Allocation of Resources Without Limits or Throttling
CWE-918	Server-Side Request Forgery (SSRF)
CWE-1023	Incomplete Comparison with Missing Factors

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
ASP.NET Core 10.0
ASP.NET Core 8.0
Microsoft.AspNetCore.OData
Visual Studio Code

Disclaimer