Nationaal Cyber Security Centrum
Ministerie van Justitie en Veiligheid

NCSC-2025-0153

Kwetsbaarheden verholpen in Microsoft Developer Tools

NCSC Advisory
Prioriteit: Normaal
Gepubliceerd op: 13-05-2025

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 volgende categorieën schade:

- Omzeilen van een beveiligingsmaatregel
- Uitvoer van willekeurige code (gebruikersrechten)
- Toegang tot gevoelige gegevens
- Spoofing
- Verkrijgen van verhoogde rechten

Voor de kwetsbaarheid met kenmerk CVE-2025-29813 heeft Microsoft inmiddels updates uitgerold binnen het Azure platform. Hiervoor zijn geen verdere acties nodig.

```
Visual Studio:
|----------------|------|-------------------------------------|
| CVE-ID         | CVSS | Impact                              |
|----------------|------|-------------------------------------|
| CVE-2025-32703 | 5.50 | Toegang tot gevoelige gegevens      |
| CVE-2025-32702 | 7.80 | Uitvoeren van willekeurige code     |
|----------------|------|-------------------------------------|

.NET, Visual Studio, and Build Tools for Visual Studio:
|----------------|------|-------------------------------------|
| CVE-ID         | CVSS | Impact                              |
|----------------|------|-------------------------------------|
| CVE-2025-26646 | 8.00 | Voordoen als andere gebruiker       |
|----------------|------|-------------------------------------|

Visual Studio Code:
|----------------|------|-------------------------------------|
| CVE-ID         | CVSS | Impact                              |
|----------------|------|-------------------------------------|
| CVE-2025-21264 | 6.70 | Omzeilen van beveiligingsmaatregel  |
|----------------|------|-------------------------------------|

Azure DevOps:
|----------------|------|-------------------------------------|
```

CVE-ID	CVSS	Impact
CVE-2025-29813	10.00	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://www.cve.org/CVERecord?id=CVE-2025-21264
- https://raw.githubusercontent.com/CVEProject/cvelistV5/main/cves/2025/21xxx/CVE-2025-21264.json
- https://www.cve.org/CVERecord?id=CVE-2025-29813
- https://raw.githubusercontent.com/CVEProject/cvelistV5/main/cves/2025/29xxx/CVE-2025-29813.json
- https://www.cve.org/CVERecord?id=CVE-2025-32702
- https://raw.githubusercontent.com/CVEProject/cvelistV5/main/cves/2025/32xxx/CVE-2025-32702.json
- https://www.cve.org/CVERecord?id=CVE-2025-32703
- https://raw.githubusercontent.com/CVEProject/cvelistV5/main/cves/2025/32xxx/CVE-2025-32703.json
- https://api.msrc.microsoft.com/cvrf/v3.0/cvrf/2025-May

Kwetsbaarheden

CVE	CVSS Score
CVE-2025-26646	
CVE-2025-32703	
CVE-2025-32702	
CVE-2025-21264	
CVE-2025-29813	10.0 CRITICAL

CWE's

CWE	Beschrijving
CWE-302	Authentication Bypass by Assumed-Immutable Data
CWE-1220	Insufficient Granularity of Access Control
CWE-77	Improper Neutralization of Special Elements used in a Command ('Command Injection')
CWE-552	Files or Directories Accessible to External Parties
CWE-200	Exposure of Sensitive Information to an Unauthorized Actor
CWE-73	External Control of File Name or Path

Getroffen producten

Microsoft
.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
Azure DevOps
Build Tools for Visual Studio 2022

Microsoft Visual Studio 2017 version 15.9 (includes 15.0 - 15.8)
Microsoft Visual Studio 2019 version 16.11 (includes 16.0 - 16.10)
Microsoft Visual Studio 2022 version 17.10
Microsoft Visual Studio 2022 version 17.12
Microsoft Visual Studio 2022 version 17.13
Microsoft Visual Studio 2022 version 17.8
Visual Studio 2019
Visual Studio 2022

Disclaimer