Nationaal Cyber Security Centrum
Ministerie van Justitie en Veiligheid

NCSC-2025-0313

Kwetsbaarheden verholpen in Microsoft Developer Tools

NCSC Advisory
Prioriteit: Normaal
Gepubliceerd op: 14-10-2025

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 zich verhoogde rechten toe te kennen, beveiligingsmaatregelen te omzeilen en toegang te krijgen tot gevoelige gegevens.

De ernstigste kwetsbaarheid heeft kenmerk CVE-2025-55315 toegewezen gekregen en bevindt zich in ASP .NET core. Een kwaadwillende kan de kwetsbaarheid misbruiken om middels http-request smuggling beveiligingsmaatregelen te omzeilen en zo toegang te krijgen tot gevoelige gegevens in de scope van de applicaties draaiend op de kwetsbare .NET core software.

```
.NET, .NET Framework, Visual Studio:
|----------------|------|-------------------------------------|
| CVE-ID         | CVSS | Impact                              |
|----------------|------|-------------------------------------|
| CVE-2025-55248 | 4.80 | Toegang tot gevoelige gegevens      |
|----------------|------|-------------------------------------|

Visual Studio:
|----------------|------|-------------------------------------|
| CVE-ID         | CVSS | Impact                              |
|----------------|------|-------------------------------------|
| CVE-2025-54132 | 4.40 | Toegang tot gevoelige gegevens      |
| CVE-2025-55240 | 7.30 | Verkrijgen van verhoogde rechten    |
|----------------|------|-------------------------------------|

Microsoft PowerShell:
|----------------|------|-------------------------------------|
| CVE-ID         | CVSS | Impact                              |
|----------------|------|-------------------------------------|
| CVE-2025-25004 | 7.30 | Verkrijgen van verhoogde rechten    |
|----------------|------|-------------------------------------|

ASP.NET Core:
|----------------|------|-------------------------------------|
| CVE-ID         | CVSS | Impact                              |
|----------------|------|-------------------------------------|
| CVE-2025-55315 | 9.90 | Omzeilen van beveiligingsmaatregel  |
```

```
|----------------|------|-----------------------------------|

.NET:
|----------------|------|-----------------------------------|
| CVE-ID         | CVSS | Impact                            |
|----------------|------|-----------------------------------|
| CVE-2025-55247 | 7.30 | 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

Kwetsbaarheden

CVE	CVSS Score
CVE-2025-25004	7.3 HIGH
CVE-2025-54132	2.1 LOW
CVE-2025-55240	7.3 HIGH
CVE-2025-55247	7.3 HIGH
CVE-2025-55248	4.8 MEDIUM
CVE-2025-55315	9.9 CRITICAL

CWE's

CWE	Beschrijving
CWE-59	Improper Link Resolution Before File Access ('Link Following')
CWE-284	Improper Access Control
CWE-326	Inadequate Encryption Strength

CWE-444	Inconsistent Interpretation of HTTP Requests ('HTTP Request/Response Smuggling')
CWE-918	Server-Side Request Forgery (SSRF)

Getroffen producten

Microsoft
.NET 8.0
.NET 9.0
ASP.NET Core 2.3
ASP.NET Core 8.0
ASP.NET Core 9.0
Microsoft .NET Framework 2.0 Service Pack 2
Microsoft .NET Framework 3.0 Service Pack 2
Microsoft .NET Framework 3.5
Microsoft .NET Framework 3.5 AND 4.7.2
Microsoft .NET Framework 3.5 AND 4.8
Microsoft .NET Framework 3.5 AND 4.8.1
Microsoft .NET Framework 3.5.1

Microsoft .NET Framework 4.6.2
Microsoft .NET Framework 4.6.2/4.7/4.7.1/4.7.2
Microsoft .NET Framework 4.8
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 17.14
PowerShell 7.4
PowerShell 7.5

Disclaimer