Nationaal Cyber Security Centrum
Ministerie van Justitie en Veiligheid

NCSC-2025-0011

Kwetsbaarheden verholpen in Microsoft Developer Tools

NCSC Advisory
Prioriteit: Normaal
Gepubliceerd op: 14-01-2025

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 Visual Studio en .NET.

Duiding

Een kwaadwillende kan de kwetsbaarheden misbruiken om zich verhoogde rechten toe te kennen, toegang te krijgen tot gevoelige gegevens of om willekeurige code uit te voeren in de context van het slachtoffer.

Voor succesvol misbruik moet de kwaadwillende het slachtoffer misleiden een malafide bestand te openen en verwerken.

Visual Studio:

CVE-ID	CVSS	Impact
CVE-2024-50338	7.40	Toegang tot gevoelige gegevens
CVE-2025-21178	8.80	Uitvoeren van willekeurige code
CVE-2025-21405	7.30	Verkrijgen van verhoogde rechten

.NET, .NET Framework, Visual Studio:

CVE-ID	CVSS	Impact
CVE-2025-21176	8.80	Uitvoeren van willekeurige code

.NET:

CVE-ID	CVSS	Impact
CVE-2025-21171	8.10	Uitvoeren van willekeurige code
CVE-2025-21173	8.00	Verkrijgen van verhoogde rechten

.NET and Visual Studio:

CVE-ID	CVSS	Impact
CVE-2025-21172	7.50	Uitvoeren van willekeurige code

|----------------|------|-----------------------------------|

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-2024-50338	
CVE-2025-21171	7.5 HIGH
CVE-2025-21172	7.5 HIGH
CVE-2025-21173	7.3 HIGH
CVE-2025-21176	8.8 HIGH
CVE-2025-21178	8.8 HIGH
CVE-2025-21405	7.3 HIGH

CWE's

CWE	Beschrijving
CWE-126	Buffer Over-read
CWE-379	Creation of Temporary File in Directory with Insecure Permissions
CWE-190	Integer Overflow or Wraparound
CWE-125	Out-of-bounds Read
CWE-284	Improper Access Control

CWE-200	Exposure of Sensitive Information to an Unauthorized Actor
CWE-122	Heap-based Buffer Overflow

Getroffen producten

microsoft
.net_8.0
.net_9.0
microsoft_.net_framework_3.5_and_4.6.2_4.7_4.7.1_4.7.2
microsoft_.net_framework_3.5_and_4.7.2
microsoft_.net_framework_3.5_and_4.8.1
microsoft_.net_framework_3.5_and_4.8
microsoft_.net_framework_4.6.2
microsoft_.net_framework_4.6.2_4.7_4.7.1_4.7.2
microsoft_.net_framework_4.6_4.6.2
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_17.6
microsoft_visual_studio_2022_version_17.8

Disclaimer