



NCSC-2024-0395

Kwetsbaarheden verholpen in Microsoft Developer Tools

NCSC Advisory

Prioriteit: Normaal

Gepubliceerd op: 08-10-2024

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 een Denial-of-Service te veroorzaken, zichzelf verhoogde rechten toe te kennen of willekeurige code uit te voeren met rechten van het slachtoffer.

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

.NET, .NET Framework, Visual Studio:

CVE-ID	CVSS	Impact
CVE-2024-43483	7.50	Denial-of-Service
CVE-2024-43484	7.50	Denial-of-Service

Visual Studio Code:

CVE-ID	CVSS	Impact
CVE-2024-43601	7.10	Uitvoeren van willekeurige code
CVE-2024-43488	8.80	Uitvoeren van willekeurige code

.NET and Visual Studio:

CVE-ID	CVSS	Impact
CVE-2024-38229	8.10	Uitvoeren van willekeurige code
CVE-2024-43485	7.50	Denial-of-Service

DeepSpeed:

CVE-ID	CVSS	Impact
CVE-2024-43497	8.40	Uitvoeren van willekeurige code

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

Visual Studio:

CVE-ID	CVSS	Impact
CVE-2024-43603	5.50	Denial-of-Service

Visual C++ Redistributable Installer:

CVE-ID	CVSS	Impact
CVE-2024-43590	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>

Kwetsbaarheden

CVE	CVSS Score
> CVE-2024-38229	8.1 HIGH
> CVE-2024-43483	7.5 HIGH
> CVE-2024-43484	7.5 HIGH
> CVE-2024-43485	7.5 HIGH
> CVE-2024-43590	7.8 HIGH
> CVE-2024-43603	5.5 MEDIUM
> CVE-2024-43601	7.1 HIGH

> CVE-2024-43488	8.8 HIGH
> CVE-2024-43497	8.4 HIGH

CWE's

CWE	Beschrijving
> CWE-59	Improper Link Resolution Before File Access ('Link Following')
> CWE-407	Inefficient Algorithmic Complexity
> CWE-77	Improper Neutralization of Special Elements used in a Command ('Command Injection')
> CWE-362	Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')
> CWE-306	Missing Authentication for Critical Function
> CWE-284	Improper Access Control
> CWE-416	Use After Free
> CWE-789	Memory Allocation with Excessive Size Value

Getroffen producten

microsoft
.net_6.0
.net_8.0
deepspeed
microsoft_.net_framework_2.0_service_pack_2
microsoft_.net_framework_3.0_service_pack_2
microsoft_.net_framework_3.5.1
microsoft_.net_framework_3.5
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_2015_update_3
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_17.11
microsoft_visual_studio_2022_version_17.6
microsoft_visual_studio_2022_version_17.8
visual_c___redistributable_installer
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.