



Advisory NCSC-2024-0283

Kwetsbaarheden verholpen in Microsoft Developer Tools

2024-07-09 Revisie 0

Toegestande verspreiding: 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 mogen de informatie delen met collega's van andere organisaties, informatiefora of personen werkzaam in netwerkbeveiliging, informatiebeveiliging of de VI-gemeenschap in de bredere zin. Het is niet de bedoeling dat u de informatie publiek maakt.

Uw reacties zijn welkom op info@ncsc.nl

Feiten

Microsoft heeft kwetsbaarheden verholpen in Visual Studio en .NET.

Interpretaties

Een kwaadwillende kan de kwetsbaarheden misbruiken om willekeurige code uit te voeren met rechten van het slachtoffer, of om een Denial-of-Service te veroorzaken.

Voor succesvol misbruik moet de kwaadwillende een race-conditie winnen.

.NET and Visual Studio:	----- ----- -----	
CVE-ID CVSS Impact	----- ----- -----	
CVE-2024-35264	8.10	Uitvoeren van willekeurige code
CVE-2024-30105	7.50	Denial-of-Service
CVE-2024-38081	7.30	Verkrijgen van verhoogde rechten
CVE-2024-38095	7.50	Denial-of-Service

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>

Dreigingsinformatie