Nationaal Cyber Security Centrum
Ministerie van Justitie en Veiligheid

NCSC-2026-0008

Kwetsbaarheid verholpen in Microsoft SQL Server

NCSC Advisory
Prioriteit: Normaal
Gepubliceerd op: 13-01-2026

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 een kwetsbaarheid verholpen in SQL Server

Duiding

Een kwaadwillende kan de kwetsbaarheid misbruiken om zonder daartoe gerechtigd te zijn toegang te krijgen tot de DEBUG-functionaliteit en daarmee, onder andere, memory-dumps genereren. Deze dumps kunnen ook betrekking hebben op geheugen buiten de scope van de SQL-server, waardoor de kwaadwillende toegang kan krijgen tot gevoelige gegevens buiten de scope van SQL-Server.

Voor succesvol misbruik moet de kwaadwillende wel beschikken over **voorafgaande verhoogde rechten** binnen SQL Server. Dit valt in principe onder een Evil-Admin scenario (insider threat). Echter, door de eenvoud van misbruik en de potentiele schade aan informatie-lekkage, adviseert het NCSC wel om deze kwetsbaarheid versneld in te zetten in infrastructuren waarbij de SQL-Server implementatie is gerealiseerd op systemen waarbij meerdere server-applicaties zijn geimplementeerd op dezelfde hardware/virtuele omgeving, zoals shared-resource-systemen en cloud-omgevingen.

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-2026-20803	7.2 HIGH

CWE's

CWE	Beschrijving
CWE-306	Missing Authentication for Critical Function

Getroffen producten

Microsoft
Microsoft SQL Server 2022 (GDR)
Microsoft SQL Server 2022 for x64-based Systems (CU 22)
Microsoft SQL Server 2022 for x64-based Systems (GDR)
Microsoft SQL Server 2025 for x64-based Systems (GDR)

Disclaimer