Nationaal Cyber Security Centrum
Ministerie van Justitie en Veiligheid

NCSC-2024-0437

Kwetsbaarheden verholpen in Microsoft SQL Server

NCSC Advisory
Prioriteit: Normaal
Gepubliceerd op: 12-11-2024

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 SQL Server.

Duiding

Een kwaadwillende kan de kwetsbaarheden misbruiken om willekeurige SQL-code uit te voeren op de database-omgeving.

Met uitzondering van de kwetsbaarheden met kenmerk CVE-2024-49021 en CVE-2024-49043 bevinden de kwetsbaarheden zich in de SQL Native Client. Succesvol misbruik van de kwetsbaarheden in de Native Client vereist dat de kwaadwillende het slachtoffer misleidt een verbinding te maken met een malafide SQL-server onder controle van de kwaadwillende.

De bovengenoemde uitzonderingen bevinden zich in de SQL-server zelf en zijn alleen lokaal te misbruiken.

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-2024-38255	
CVE-2024-43459	8.8 HIGH
CVE-2024-43462	8.8 HIGH
CVE-2024-48994	8.8 HIGH
CVE-2024-48995	8.8 HIGH
CVE-2024-48996	
CVE-2024-49043	

CVE-2024-48993	
CVE-2024-48997	
CVE-2024-48998	8.8 HIGH
CVE-2024-48999	
CVE-2024-49000	8.8 HIGH
CVE-2024-49001	
CVE-2024-49002	
CVE-2024-49003	
CVE-2024-49004	8.8 HIGH
CVE-2024-49005	
CVE-2024-49007	8.8 HIGH
CVE-2024-49006	
CVE-2024-49008	8.8 HIGH
CVE-2024-49009	8.8 HIGH
CVE-2024-49010	8.8 HIGH
CVE-2024-49011	
CVE-2024-49012	
CVE-2024-49013	
CVE-2024-49014	
CVE-2024-49015	
CVE-2024-49016	
CVE-2024-49017	8.8 HIGH
CVE-2024-49018	8.8 HIGH

- CVE-2024-49021

CWE's

CWE	Beschrijving
CWE-415	Double Free
CWE-426	Untrusted Search Path
CWE-416	Use After Free
CWE-122	Heap-based Buffer Overflow

Getroffen producten

microsoft
sql_server

Disclaimer