Nationaal Cyber Security Centrum
Ministerie van Justitie en Veiligheid

NCSC-2025-0247

Kwetsbaarheden verholpen in Microsoft SQL Server

NCSC Advisory
Prioriteit: Normaal
Gepubliceerd op: 13-08-2025

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 SQL Server.

Duiding

De kwetsbaarheden zijn gerelateerd aan onjuist toegangsbeheer en SQL-injectie, waardoor geautoriseerde aanvallers hun privileges binnen een netwerk kunnen escaleren. Dit kan leiden tot ongeautoriseerde toegang en manipulatie van gevoelige gegevens. De kwetsbaarheden zijn aanwezig in meerdere versies van SQL Server, waarbij de ernst kan variëren op basis van specifieke configuraties en implementaties.

```
SQL Server:
|----------------|------|-----------------------------------|
| CVE-ID         | CVSS | Impact                            |
|----------------|------|-----------------------------------|
| CVE-2025-49758 | 8.80 | Verkrijgen van verhoogde rechten  |
| CVE-2025-53727 | 8.80 | Verkrijgen van verhoogde rechten  |
| CVE-2025-24999 | 8.80 | Verkrijgen van verhoogde rechten  |
| CVE-2025-49759 | 8.80 | Verkrijgen van verhoogde rechten  |
| CVE-2025-47954 | 8.80 | Verkrijgen van verhoogde rechten  |
|----------------|------|-----------------------------------|
```

Oplossingen

Microsoft heeft updates uitgebracht om de kwetsbaarheden te verhelpen. Zie bijgevoegde referenties voor meer informatie.

Referenties

- https://msrc.microsoft.com/update-guide/en-us

Kwetsbaarheden

CVE	CVSS Score
CVE-2025-24999	8.8 HIGH
CVE-2025-47954	8.8 HIGH
CVE-2025-49758	

CVE-2025-49759	8.8 HIGH
CVE-2025-53727	

CWE's

CWE	Beschrijving
CWE-284	Improper Access Control
CWE-89	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')
CWE-269	Improper Privilege Management

Getroffen producten

Microsoft
Microsoft SQL Server 2019 for x64-based Systems (CU 32)
Microsoft SQL Server 2022 for x64-based Systems (CU 20)
Microsoft SQL Server 2022 for x64-based Systems (GDR)
Microsoft SQL Server 2017 for x64-based Systems (CU 31)
Microsoft SQL Server 2017 for x64-based Systems (GDR)
Microsoft SQL Server 2016 for x64-based Systems Service Pack 3 (GDR)
Microsoft SQL Server 2016 Service Pack 3 Azure Connect Feature Pack
Microsoft SQL Server 2016 Service Pack 3 (GDR)

Microsoft SQL Server 2019 (GDR)
Microsoft SQL Server 2017 (GDR)
sql_server
Sql_Server_2022
Sql_Server_2019
Sql_Server_2016
Microsoft SQL Server 2017 (CU 31)

Disclaimer