



NCSC-2024-0364

Kwetsbaarheden verholpen in Microsoft SQL Server

NCSC Advisory

Prioriteit: Normaal

Gepubliceerd op: 10-09-2024

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

De meeste kwetsbaarheden bevinden zich in SQL Native Scoring en stellen een kwaadwillende in staat om zich verhoogde rechten toe te kennen, toegang te krijgen tot gevoelige gegevens en willekeurige code uit te voeren binnen de SQL Server.

Voor succesvol misbruik moet de kwaadwillende over voorafgaande authenticatie beschikken.

SQL Server:

CVE-ID	CVSS	Impact
CVE-2024-37338	8.80	Uitvoeren van willekeurige code
CVE-2024-37966	7.10	Toegang tot gevoelige gegevens
CVE-2024-37335	8.80	Uitvoeren van willekeurige code
CVE-2024-37340	8.80	Uitvoeren van willekeurige code
CVE-2024-37339	8.80	Uitvoeren van willekeurige code
CVE-2024-37337	7.10	Toegang tot gevoelige gegevens
CVE-2024-37342	7.10	Toegang tot gevoelige gegevens
CVE-2024-26186	8.80	Uitvoeren van willekeurige code
CVE-2024-26191	8.80	Uitvoeren van willekeurige code
CVE-2024-43474	7.60	Toegang tot gevoelige gegevens
CVE-2024-37965	8.80	Verkrijgen van verhoogde rechten
CVE-2024-37341	8.80	Verkrijgen van verhoogde rechten
CVE-2024-37980	8.80	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-2024-37338	8.8 HIGH
> CVE-2024-37966	7.1 HIGH
> CVE-2024-37335	
> CVE-2024-37340	
> CVE-2024-37339	
> CVE-2024-37337	7.1 HIGH
> CVE-2024-37342	7.1 HIGH
> CVE-2024-26186	
> CVE-2024-26191	8.8 HIGH
> CVE-2024-43474	
> CVE-2024-37965	8.8 HIGH
> CVE-2024-37341	8.8 HIGH
> CVE-2024-37980	

CWE's

CWE	Beschrijving
> CWE-197	Numeric Truncation Error
> CWE-170	Improper Null Termination
> CWE-822	Untrusted Pointer Dereference
> CWE-125	Out-of-bounds Read
> CWE-284	Improper Access Control
> CWE-416	Use After Free

➤ CWE-122	Heap-based Buffer Overflow
➤ CWE-269	Improper Privilege Management
➤ CWE-20	Improper Input Validation

Getroffen producten

microsoft
microsoft_sql_server_2016_service_pack_3_gdr_
microsoft_sql_server_2016_service_pack_3_azure_connect_feature_pack
microsoft_sql_server_2017__cu_31_
microsoft_sql_server_2017__gdr_
microsoft_sql_server_2019__cu_28_
microsoft_sql_server_2019__gdr_
microsoft_sql_server_2022__gdr_
microsoft_sql_server_2022_for__cu_14_

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.