



NCSC-2024-0281

Kwetsbaarheden verholpen in Microsoft Windows SQL Server

NCSC Advisory

Prioriteit: Normaal

Gepubliceerd op: 09-07-2024

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 Windows SQL Server.

Duiding

De kwetsbaarheden bevinden zich in de Native Client van SQL Server en stellen een kwaadwillende in staat om willekeurige code uit te voeren in de context van het slachtoffer en zo mogelijk toegang krijgen tot gevoelige gegevens in Database-omgevingen waar het slachtoffer toegang toe heeft.

Voor succesvol misbruik moet de kwaadwillende het slachtoffer misleiden om contact te maken met een SQL server onder controle van de kwaadwillende.

SQL Server:

CVE-ID	CVSS	Impact
CVE-2024-38088	8.80	Uitvoeren van willekeurige code
CVE-2024-38087	8.80	Uitvoeren van willekeurige code
CVE-2024-21332	8.80	Uitvoeren van willekeurige code
CVE-2024-21333	8.80	Uitvoeren van willekeurige code
CVE-2024-21335	8.80	Uitvoeren van willekeurige code
CVE-2024-21373	8.80	Uitvoeren van willekeurige code
CVE-2024-21398	8.80	Uitvoeren van willekeurige code
CVE-2024-21414	8.80	Uitvoeren van willekeurige code
CVE-2024-21415	8.80	Uitvoeren van willekeurige code
CVE-2024-21428	8.80	Uitvoeren van willekeurige code
CVE-2024-37318	8.80	Uitvoeren van willekeurige code
CVE-2024-37332	8.80	Uitvoeren van willekeurige code
CVE-2024-37331	8.80	Uitvoeren van willekeurige code
CVE-2024-35271	8.80	Uitvoeren van willekeurige code
CVE-2024-35272	8.80	Uitvoeren van willekeurige code
CVE-2024-20701	8.80	Uitvoeren van willekeurige code
CVE-2024-21303	8.80	Uitvoeren van willekeurige code
CVE-2024-21308	8.80	Uitvoeren van willekeurige code
CVE-2024-21317	8.80	Uitvoeren van willekeurige code
CVE-2024-21331	8.80	Uitvoeren van willekeurige code
CVE-2024-21425	8.80	Uitvoeren van willekeurige code
CVE-2024-37319	8.80	Uitvoeren van willekeurige code
CVE-2024-37320	8.80	Uitvoeren van willekeurige code
CVE-2024-37321	8.80	Uitvoeren van willekeurige code

CVE-2024-37322	8.80	Uitvoeren van willekeurige code	
CVE-2024-37323	8.80	Uitvoeren van willekeurige code	
CVE-2024-37324	8.80	Uitvoeren van willekeurige code	
CVE-2024-21449	8.80	Uitvoeren van willekeurige code	
CVE-2024-37326	8.80	Uitvoeren van willekeurige code	
CVE-2024-37327	8.80	Uitvoeren van willekeurige code	
CVE-2024-37328	8.80	Uitvoeren van willekeurige code	
CVE-2024-37329	8.80	Uitvoeren van willekeurige code	
CVE-2024-37330	8.80	Uitvoeren van willekeurige code	
CVE-2024-37334	8.80	Uitvoeren van willekeurige code	
CVE-2024-37333	8.80	Uitvoeren van willekeurige code	
CVE-2024-37336	8.80	Uitvoeren van willekeurige code	
CVE-2024-28928	8.80	Uitvoeren van willekeurige code	
CVE-2024-35256	8.80	Uitvoeren van willekeurige code	
----- ----- -----			

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

Kwetsbaarheden

CVE	CVSS Score
> CVE-2024-38087	8.8 HIGH
> CVE-2024-21332	8.8 HIGH
> CVE-2024-21333	8.8 HIGH
> CVE-2024-21335	8.8 HIGH
> CVE-2024-21373	8.8 HIGH
> CVE-2024-21398	8.8 HIGH

> CVE-2024-21414	8.8 HIGH
> CVE-2024-21415	8.8 HIGH
> CVE-2024-21428	8.8 HIGH
> CVE-2024-37318	8.8 HIGH
> CVE-2024-37332	8.8 HIGH
> CVE-2024-37331	8.8 HIGH
> CVE-2024-35271	
> CVE-2024-35272	
> CVE-2024-20701	8.8 HIGH
> CVE-2024-21303	8.8 HIGH
> CVE-2024-21308	8.8 HIGH
> CVE-2024-21317	8.8 HIGH
> CVE-2024-21331	
> CVE-2024-21425	
> CVE-2024-37319	
> CVE-2024-37320	8.8 HIGH
> CVE-2024-37321	8.8 HIGH
> CVE-2024-37322	
> CVE-2024-37323	
> CVE-2024-37324	
> CVE-2024-21449	8.8 HIGH
> CVE-2024-37326	8.8 HIGH
> CVE-2024-37327	8.8 HIGH

> CVE-2024-37328	
> CVE-2024-37329	
> CVE-2024-37330	8.8 HIGH
> CVE-2024-37334	8.8 HIGH
> CVE-2024-37333	
> CVE-2024-37336	
> CVE-2024-28928	
> CVE-2024-35256	
> CVE-2024-38088	8.8 HIGH

CWE's

CWE	Beschrijving
> CVE-121	Stack-based Buffer Overflow
> CVE-122	Heap-based Buffer Overflow
> CVE-190	Integer Overflow or Wraparound
> CVE-415	Double Free
> CVE-416	Use After Free

Getroffen producten

microsoft
microsoft_ole_db_driver_18_for_sql_server
microsoft_ole_db_driver_19_for_sql_server
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__gdr_
microsoft_sql_server_2019_for_x64-based_systems__cu_27_
microsoft_sql_server_2022__gdr_
microsoft_sql_server_2022_for__cu_13_
sql_server

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.