



Advisory NCSC-2026-0420

PRIORITEIT: NORMAAL

Kwetsbaarheden verholpen in Microsoft SQL Server

Publicatiedatum: 13-10-2026

Toegestane verspreiding: TLP:WHITE
(Traffic Light Protocol)

Deze publicatie bevat het label TLP:WHITE en wordt door het Nationaal Cyber Security Center (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.

Reacties zijn welkom op info@ncsc.nl.

Feiten

Microsoft heeft kwetsbaarheden verholpen in SQL Server.

Duiding

Een kwaadwillende kan de kwetsbaarheden misbruiken om een Denial-of-Service te veroorzaken, zich verhoogde rechten toe te kennen, willekeurige code uit te voeren, mogelijk met rechten van de SQL server en toegang te krijgen tot gevoelige gegevens.

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-2026-65674	
CVE-2026-67625	
CVE-2026-67626	
CVE-2026-67628	
CVE-2026-68883	
CVE-2026-70189	
CVE-2026-83945	
CVE-2026-85876	
CVE-2026-85886	
CVE-2026-85888	
CVE-2026-85919	
CVE-2026-88081	

CVE	CVSS Score
CVE-2026-88082	
CVE-2026-88083	
CVE-2026-88084	
CVE-2026-88085	
CVE-2026-88086	
CVE-2026-88088	
CVE-2026-88089	
CVE-2026-94512	
CVE-2026-94520	
CVE-2026-96956	

CWE's

CWE	Beschrijving
CWE-121	Stack-based Buffer Overflow
CWE-122	Heap-based Buffer Overflow
CWE-125	Out-of-bounds Read
CWE-134	Use of Externally-Controlled Format String
CWE-190	Integer Overflow or Wraparound
CWE-416	Use After Free
CWE-502	Deserialization of Untrusted Data
CWE-770	Allocation of Resources Without Limits or Throttling

Getroffen producten

Microsoft

Azure API Center

Microsoft SQL Server 2017 for x64-based Systems (GDR)

Microsoft SQL Server 2019 for x64-based Systems (GDR)

Microsoft SQL Server 2022 for x64-based Systems (CU 26)

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

Microsoft SQL Server 2025 for x64-based Systems (CU8)

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

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 or 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.