Nationaal Cyber Security Centrum
Ministerie van Justitie en Veiligheid

Advisory NCSC-2026-0476

PRIORITEIT: NORMAAL

Kwetsbaarheden verholpen in Microsoft SQL Server

Publicatiedatum: 10-11-2026

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 de-len. 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 55 kwetsbaarheden verholpen in diverse componenten van SQL Server.

Duiding

Een kwaadwillende kan de kwetsbaarheden misbruiken om aanvallen uit te voeren die kunnen leiden tot de categorieën schade zoals benoemd in onderstaande tabel.

De kwetsbaarheid met kenmerk CVE-2026-116945, heeft een CVSS-score van 9.8 en betreft een heap-based buffer overflow in Microsoft SQL Server. Een ongeautoriseerde kwaadwillende die controle heeft over een netwerkeindpunt waarmee een kwetsbaar integratiepakket verbinding maakt, kan een speciaal geprepareerd antwoord terugsturen. Wanneer het integratiepakket dit antwoord verwerkt, kan de kwaadwillende willekeurige code uitvoeren met de rechten van de integratieservice.

SQL Server:

CVE-ID	CVSS	Impact
CVE-2026-116929	7,50	Verkrijgen van verhoogde rechten
CVE-2026-116930	8,80	Uitvoeren van willekeurige code
CVE-2026-116931	7,50	Uitvoeren van willekeurige code
CVE-2026-116932	6,50	Toegang tot gevoelige gegevens
CVE-2026-116933	7,20	Uitvoeren van willekeurige code
CVE-2026-116934	8,80	Verkrijgen van verhoogde rechten
CVE-2026-116935	6,50	Toegang tot gevoelige gegevens
CVE-2026-116936	7,20	Uitvoeren van willekeurige code
CVE-2026-116937	7,50	Uitvoeren van willekeurige code
CVE-2026-116938	7,50	Uitvoeren van willekeurige code
CVE-2026-116939	5,70	Toegang tot gevoelige gegevens
CVE-2026-116940	4,90	Toegang tot gevoelige gegevens
CVE-2026-116941	8,80	Uitvoeren van willekeurige code
CVE-2026-116942	8,80	Uitvoeren van willekeurige code
CVE-2026-116943	7,50	Toegang tot gevoelige gegevens
CVE-2026-116944	7,20	Verkrijgen van verhoogde rechten
CVE-2026-116945	9,80	Uitvoeren van willekeurige code
CVE-2026-116946	8,80	Uitvoeren van willekeurige code
CVE-2026-116947	7,50	Uitvoeren van willekeurige code
CVE-2026-118102	5,90	Toegang tot gevoelige gegevens
CVE-2026-118103	6,50	Toegang tot gevoelige gegevens
CVE-2026-118104	6,50	Toegang tot gevoelige gegevens
CVE-2026-118105	8,80	Verkrijgen van verhoogde rechten
CVE-2026-118106	8,10	Uitvoeren van willekeurige code
CVE-2026-118108	7,50	Verkrijgen van verhoogde rechten
CVE-2026-118109	8,80	Verkrijgen van verhoogde rechten
CVE-2026-118110	8,80	Verkrijgen van verhoogde rechten
CVE-2026-118111	8,00	Verkrijgen van verhoogde rechten
CVE-2026-118112	8,00	Verkrijgen van verhoogde rechten
CVE-2026-118113	8,00	Verkrijgen van verhoogde rechten
CVE-2026-118114	7,50	Verkrijgen van verhoogde rechten
CVE-2026-118115	7,50	Verkrijgen van verhoogde rechten

CVE-2026-118116	7,00	Verkrijgen van verhoogde rechten
CVE-2026-118117	8,00	Verkrijgen van verhoogde rechten
CVE-2026-118118	8,00	Verkrijgen van verhoogde rechten
CVE-2026-118119	8,00	Verkrijgen van verhoogde rechten
CVE-2026-118120	8,80	Verkrijgen van verhoogde rechten
CVE-2026-45478	7,80	Verkrijgen van verhoogde rechten
CVE-2026-62903	onb.	Toegang tot gevoelige gegevens
CVE-2026-66813	8,10	Verkrijgen van verhoogde rechten
CVE-2026-67372	onb.	Uitvoeren van willekeurige code
CVE-2026-67374	8,80	Uitvoeren van willekeurige code
CVE-2026-67382	6,50	Toegang tot gevoelige gegevens
CVE-2026-67387	8,80	Verkrijgen van verhoogde rechten
CVE-2026-67391	8,80	Uitvoeren van willekeurige code
CVE-2026-67632	8,80	Uitvoeren van willekeurige code
CVE-2026-67637	8,80	Uitvoeren van willekeurige code
CVE-2026-67646	onb.	Uitvoeren van willekeurige code
CVE-2026-68783	onb.	Toegang tot gevoelige gegevens
CVE-2026-84010	7,50	Verkrijgen van verhoogde rechten
CVE-2026-88111	7,50	Uitvoeren van willekeurige code
CVE-2026-94511	8,80	Uitvoeren van willekeurige code
CVE-2026-94513	8,00	Verkrijgen van verhoogde rechten

JDBC Driver for SQL Server:

CVE-ID	CVSS	Impact
CVE-2026-70003	8,70	Omzeilen van beveiligingsmaatregel

Microsoft Azure Kubernetes Service:

CVE-ID	CVSS	Impact
CVE-2026-69893	onb.	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

Referenties

- https://portal.msrc.microsoft.com/en-us/security-guidance

Kwetsbaarheden

CVE	CVSS Score
CVE-2026-116929	7.5 HIGH
CVE-2026-116930	8.8 HIGH
CVE-2026-116931	7.5 HIGH
CVE-2026-116932	6.5 MEDIUM
CVE-2026-116933	7.2 HIGH
CVE-2026-116934	8.8 HIGH
CVE-2026-116935	6.5 MEDIUM
CVE-2026-116936	7.2 HIGH
CVE-2026-116937	7.5 HIGH
CVE-2026-116938	7.5 HIGH
CVE-2026-116939	5.7 MEDIUM
CVE-2026-116940	4.9 MEDIUM
CVE-2026-116941	8.8 HIGH
CVE-2026-116942	8.8 HIGH
CVE-2026-116943	7.5 HIGH
CVE-2026-116944	7.2 HIGH
CVE-2026-116945	9.8 CRITICAL
CVE-2026-116946	8.8 HIGH
CVE-2026-116947	7.5 HIGH
CVE-2026-118102	5.9 MEDIUM
CVE-2026-118103	6.5 MEDIUM
CVE-2026-118104	6.5 MEDIUM
CVE-2026-118105	8.8 HIGH

CVE	CVSS Score
CVE-2026-118106	8.1 HIGH
CVE-2026-118108	7.5 HIGH
CVE-2026-118109	8.8 HIGH
CVE-2026-118110	8.8 HIGH
CVE-2026-118111	8.0 HIGH
CVE-2026-118112	8.0 HIGH
CVE-2026-118113	8.0 HIGH
CVE-2026-118114	7.5 HIGH
CVE-2026-118115	7.5 HIGH
CVE-2026-118116	7.0 HIGH
CVE-2026-118117	8.0 HIGH
CVE-2026-118118	8.0 HIGH
CVE-2026-118119	8.0 HIGH
CVE-2026-118120	8.8 HIGH
CVE-2026-45478	
CVE-2026-62903	7.4 HIGH
CVE-2026-66813	8.1 HIGH
CVE-2026-67372	8.8 HIGH
CVE-2026-67374	8.8 HIGH
CVE-2026-67382	6.5 MEDIUM
CVE-2026-67387	8.8 HIGH
CVE-2026-67391	8.8 HIGH
CVE-2026-67632	8.8 HIGH
CVE-2026-67637	8.8 HIGH
CVE-2026-67646	8.8 HIGH
CVE-2026-68783	6.5 MEDIUM
CVE-2026-69893	
CVE-2026-70003	8.7 HIGH
CVE-2026-84010	7.5 HIGH
CVE-2026-88111	7.5 HIGH
CVE-2026-94511	8.8 HIGH

CVE	CVSS Score
CVE-2026-94513	8.0 HIGH

CWE's

CWE	Beschrijving
CWE-22	Improper Limitation of a Pathname to a Restricted Directory
CWE-77	Improper Neutralization of Special Elements used in a Command
CWE-89	Improper Neutralization of Special Elements used in an SQL Command
CWE-94	Improper Control of Generation of Code
CWE-121	Stack-based Buffer Overflow
CWE-122	Heap-based Buffer Overflow
CWE-125	Out-of-bounds Read
CWE-126	Buffer Over-read
CWE-250	Execution with Unnecessary Privileges
CWE-266	Incorrect Privilege Assignment
CWE-294	Authentication Bypass by Capture-replay
CWE-327	Use of a Broken or Risky Cryptographic Algorithm
CWE-346	Origin Validation Error
CWE-347	Improper Verification of Cryptographic Signature
CWE-749	Exposed Dangerous Method or Function
CWE-822	Untrusted Pointer Dereference
CWE-908	Use of Uninitialized Resource

Getroffen producten

Microsoft
Microsoft JDBC Driver 13.4 for SQL Server
Microsoft SQL Server 2017 for x64-based Systems (CU31)
Microsoft SQL Server 2017 for x64-based Systems (GDR)
Microsoft SQL Server 2019 for x64-based Systems (CU32)
Microsoft SQL Server 2019 for x64-based Systems (GDR)
Microsoft SQL Server 2022 for x64-based Systems (CU27)
Microsoft SQL Server 2022 for x64-based Systems (GDR)
Microsoft SQL Server 2025 for x64-based Systems (CU10)
Microsoft SQL Server 2025 for x64-based Systems (CU9)
Microsoft SQL Server 2025 for x64-based Systems (GDR)
Microsoft SQL Server Integration Services on Windows
Microsoft.Data.SqlClient 6.1
Microsoft.Data.SqlClient 7.0
Microsoft.Data.SqlClient 7.1
azurefile-csi-driver

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.