Nationaal Cyber Security Centrum
*Ministerie van Justitie en Veiligheid*

# NCSC-2026-0350

## Kwetsbaarheden verholpen in SQL Server

NCSC Security Advisory
Prioriteit: Normaal
Gepubliceerd op: 08-09-2026

**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 62 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.

SQL Server:

| CVE-ID | CVSS | Impact |
|---|---|---|
| CVE-2026-47297 | 8,10 | Uitvoeren van willekeurige code |
| CVE-2026-66814 | 8,80 | Verkrijgen van verhoogde rechten |
| CVE-2026-66816 | 6,50 | Omzeilen van beveiligingsmaatregel |
| CVE-2026-66818 | 8,80 | Verkrijgen van verhoogde rechten |
| CVE-2026-66819 | 8,80 | Verkrijgen van verhoogde rechten |
| CVE-2026-66820 | 8,80 | Verkrijgen van verhoogde rechten |
| CVE-2026-67368 | 8,80 | Verkrijgen van verhoogde rechten |
| CVE-2026-67369 | 6,50 | Toegang tot gevoelige gegevens |
| CVE-2026-67370 | 8,80 | Verkrijgen van verhoogde rechten |
| CVE-2026-67373 | 8,80 | Uitvoeren van willekeurige code |
| CVE-2026-67376 | 7,50 | Denial-of-Service |
| CVE-2026-67378 | 8,50 | Uitvoeren van willekeurige code |
| CVE-2026-67379 | 8,50 | Uitvoeren van willekeurige code |
| CVE-2026-67380 | 8,80 | Uitvoeren van willekeurige code |
| CVE-2026-67381 | 8,80 | Verkrijgen van verhoogde rechten |
| CVE-2026-67383 | 6,50 | Toegang tot gevoelige gegevens |
| CVE-2026-67384 | 8,80 | Uitvoeren van willekeurige code |
| CVE-2026-67385 | 8,80 | Uitvoeren van willekeurige code |
| CVE-2026-67386 | 6,50 | Toegang tot gevoelige gegevens |
| CVE-2026-67388 | 8,80 | Uitvoeren van willekeurige code |
| CVE-2026-67389 | 6,50 | Toegang tot gevoelige gegevens |
| CVE-2026-67390 | 6,50 | Toegang tot gevoelige gegevens |
| CVE-2026-67393 | 6,50 | Toegang tot gevoelige gegevens |
| CVE-2026-67624 | 6,50 | Toegang tot gevoelige gegevens |
| CVE-2026-67629 | 6,50 | Toegang tot gevoelige gegevens |
| CVE-2026-67630 | 6,50 | Toegang tot gevoelige gegevens |
| CVE-2026-67631 | 8,80 | Uitvoeren van willekeurige code |
| CVE-2026-67633 | 6,50 | Denial-of-Service |

| CVE-2026-67636 | 8,50 | Uitvoeren van willekeurige code |
| CVE-2026-67638 | 8,80 | Uitvoeren van willekeurige code |
| CVE-2026-67639 | 8,80 | Uitvoeren van willekeurige code |
| CVE-2026-67641 | 6,50 | Denial-of-Service |
| CVE-2026-67642 | 8,80 | Uitvoeren van willekeurige code |
| CVE-2026-67643 | 8,80 | Uitvoeren van willekeurige code |
| CVE-2026-67645 | 6,50 | Toegang tot gevoelige gegevens |
| CVE-2026-67648 | 6,50 | Toegang tot gevoelige gegevens |
| CVE-2026-68775 | 8,80 | Uitvoeren van willekeurige code |
| CVE-2026-68776 | 6,50 | Toegang tot gevoelige gegevens |
| CVE-2026-68777 | 6,50 | Toegang tot gevoelige gegevens |
| CVE-2026-68778 | 6,50 | Toegang tot gevoelige gegevens |
| CVE-2026-68779 | 6,50 | Toegang tot gevoelige gegevens |
| CVE-2026-68780 | 6,50 | Toegang tot gevoelige gegevens |
| CVE-2026-68781 | 6,50 | Toegang tot gevoelige gegevens |
| CVE-2026-68784 | 6,50 | Toegang tot gevoelige gegevens |
| CVE-2026-68785 | 4,90 | Uitvoeren van willekeurige code |
| CVE-2026-68786 | 8,80 | Uitvoeren van willekeurige code |
| CVE-2026-68787 | 7,80 | Uitvoeren van willekeurige code |
| CVE-2026-69562 | 6,50 | Toegang tot gevoelige gegevens |
| CVE-2026-73028 | 8,80 | Verkrijgen van verhoogde rechten |
| CVE-2026-73029 | 6,50 | Toegang tot gevoelige gegevens |
| CVE-2026-77480 | 8,80 | Verkrijgen van verhoogde rechten |
| CVE-2026-77481 | 8,80 | Uitvoeren van willekeurige code |
| CVE-2026-77482 | 8,80 | Uitvoeren van willekeurige code |
| CVE-2026-77483 | 8,80 | Verkrijgen van verhoogde rechten |
| CVE-2026-77484 | 8,80 | Uitvoeren van willekeurige code |
| CVE-2026-77485 | 7,00 | Verkrijgen van verhoogde rechten |
| CVE-2026-77486 | 8,80 | Uitvoeren van willekeurige code |
| CVE-2026-77487 | 8,80 | Verkrijgen van verhoogde rechten |
| CVE-2026-77488 | 5,50 | Toegang tot gevoelige gegevens |
| CVE-2026-78456 | 8,80 | Uitvoeren van willekeurige code |

Windows OLE DB:

| CVE-ID | CVSS | Impact |
| --- | --- | --- |
| CVE-2026-78441 | 6,50 | Toegang tot gevoelige gegevens |
| CVE-2026-78442 | 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

## Referenties

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

## Kwetsbaarheden

| CVE | CVSS Score |
| --- | --- |
| CVE-2026-47297 | |
| CVE-2026-66814 | |
| CVE-2026-66816 | |
| CVE-2026-66818 | |
| CVE-2026-66819 | |
| CVE-2026-66820 | |
| CVE-2026-67368 | |
| CVE-2026-67369 | |
| CVE-2026-67370 | |
| CVE-2026-67373 | |
| CVE-2026-67376 | |
| CVE-2026-67378 | |
| CVE-2026-67379 | |
| CVE-2026-67380 | |

- CVE-2026-67381
- CVE-2026-67383
- CVE-2026-67384
- CVE-2026-67385
- CVE-2026-67386
- CVE-2026-67388
- CVE-2026-67389
- CVE-2026-67390
- CVE-2026-67393
- CVE-2026-67624
- CVE-2026-67629
- CVE-2026-67630
- CVE-2026-67631
- CVE-2026-67633
- CVE-2026-67636
- CVE-2026-67638
- CVE-2026-67639
- CVE-2026-67641
- CVE-2026-67642
- CVE-2026-67643
- CVE-2026-67645
- CVE-2026-67648
- CVE-2026-68775

- CVE-2026-68776
- CVE-2026-68777
- CVE-2026-68778
- CVE-2026-68779
- CVE-2026-68780
- CVE-2026-68781
- CVE-2026-68784
- CVE-2026-68785
- CVE-2026-68786
- CVE-2026-68787
- CVE-2026-69562
- CVE-2026-73028
- CVE-2026-73029
- CVE-2026-77480
- CVE-2026-77481
- CVE-2026-77482
- CVE-2026-77483
- CVE-2026-77484
- CVE-2026-77485
- CVE-2026-77486
- CVE-2026-77487
- CVE-2026-77488
- CVE-2026-78441

- CVE-2026-78442
- CVE-2026-78456

## CWE's

| CWE | Beschrijving |
|---|---|
| CWE-59 | Improper Link Resolution Before File Access ('Link Following') |
| CWE-89 | Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') |
| CWE-121 | Stack-based Buffer Overflow |
| CWE-122 | Heap-based Buffer Overflow |
| CWE-125 | Out-of-bounds Read |
| CWE-126 | Buffer Over-read |
| CWE-190 | Integer Overflow or Wraparound |
| CWE-191 | Integer Underflow (Wrap or Wraparound) |
| CWE-209 | Generation of Error Message Containing Sensitive Information |
| CWE-416 | Use After Free |
| CWE-502 | Deserialization of Untrusted Data |
| CWE-778 | Insufficient Logging |
| CWE-822 | Untrusted Pointer Dereference |
| CWE-908 | Use of Uninitialized Resource |
| CWE-1220 | Insufficient Granularity of Access Control |
| CWE-1390 | Weak Authentication |

## Getroffen producten

| **Microsoft** |
| --- |
| Microsoft OLE DB Driver 19 for SQL Server |
| Microsoft SQL Server 2017 for x64-based Systems (CU 31) |
| Microsoft SQL Server 2017 for x64-based Systems (GDR) |
| Microsoft SQL Server 2019 for x64-based Systems (CU 32) |
| Microsoft SQL Server 2019 for x64-based Systems (GDR) |
| Microsoft SQL Server 2022 for x64-based Systems (CU 25) |
| 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 (CU6) |
| Microsoft SQL Server 2025 for x64-based Systems (CU8) |
| Microsoft SQL Server 2025 for x64-based Systems (GDR) |
| Microsoft SQL Server Integration Services |

## Disclaimer