



# SQL Server Elevation of Privilege Vulnerability

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF](#) 

## Summary

|                        |                                                                                                                             |
|------------------------|-----------------------------------------------------------------------------------------------------------------------------|
| <b>CVE</b>             | CVE-2026-32176                                                                                                              |
| <b>State</b>           | PUBLISHED                                                                                                                   |
| <b>Assigner</b>        | microsoft                                                                                                                   |
| <b>Source Priority</b> | CVE Program / NVD first with legacy fallback                                                                                |
| <b>Published</b>       | 2026-04-14 18:17:20 UTC                                                                                                     |
| <b>Updated</b>         | 2026-05-07 19:52:49 UTC                                                                                                     |
| <b>Description</b>     | Improper neutralization of special elements used in an sql command ('sql injection') in SQL Server allows an authorized att |

## Risk And Classification

**Primary CVSS:** v3.1 7.8 HIGH from nvd@nist.gov

**CVSS:** 3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

**EPSS:** 0.000690000 probability, percentile 0.211320000 (date 2026-04-21)

**Problem Types:** CWE-89 | CWE-89 CWE-89: Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')

| Version | Source               | Type      | Score | Severity | Vector                                                     |
|---------|----------------------|-----------|-------|----------|------------------------------------------------------------|
| 3.1     | nvd@nist.gov         | Primary   | 7.8   | HIGH     | CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H               |
| 3.1     | secure@microsoft.com | Secondary | 6.7   | MEDIUM   | CVSS:3.1/AV:L/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:H               |
| 3.1     | CNA                  | CVSS      | 6.7   | MEDIUM   | CVSS:3.1/AV:L/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C |

## CVSS v3.1 Breakdown

Attack Vector

Local

Attack Complexity

Low

Privileges Required

Low

User Interaction

None

Scope

Unchanged

Confidentiality

High

Integrity

High

Availability

High

CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

### NVD Known Affected Configurations (CPE 2.3)

| Type        | Vendor    | Product         | Version | Update | Edition | Language |
|-------------|-----------|-----------------|---------|--------|---------|----------|
| Application | Microsoft | Sql Server 2016 | All     | All    | All     | All      |

### Vendor Declared Affected Products

| Source | Vendor    | Product                                                             | Version                                 |
|--------|-----------|---------------------------------------------------------------------|-----------------------------------------|
| CNA    | Microsoft | Microsoft SQL Server 2016 Service Pack 3 GDR                        | affected 13.0.0 13.0.6485.1 custom      |
| CNA    | Microsoft | Microsoft SQL Server 2016 Service Pack 3 Azure Connect Feature Pack | affected 13.0.0 13.0.7080.1 custom      |
| CNA    | Microsoft | Microsoft SQL Server 2017 CU 31                                     | affected 14.0.0 14.0.3525.1 custom      |
| CNA    | Microsoft | Microsoft SQL Server 2017 GDR                                       | affected 14.0.0 14.0.2105.1 custom      |
| CNA    | Microsoft | Microsoft SQL Server 2019 CU 32                                     | affected 15.0.0.0 15.0.4465.1 custom    |
| CNA    | Microsoft | Microsoft SQL Server 2019 GDR                                       | affected 15.0.0 15.0.2165.1 custom      |
| CNA    | Microsoft | Microsoft SQL Server 2022 GDR                                       | affected 16.0.0 16.0.1175.1 custom      |
| CNA    | Microsoft | Microsoft SQL Server 2022 For X64-based Systems CU 24               | affected 16.0.0.0 16.0.4250.1 custom    |
| CNA    | Microsoft | Microsoft SQL Server 2025 CU 3                                      | affected 17.0.4030.1 17.0.4030.1 custom |
| CNA    | Microsoft | Microsoft SQL Server 2025 For X64-based Systems GDR                 | affected 17.0.1050.2 17.0.1110.1 custom |

### References

| Reference                                                                                                                                       | Source               | Link                                                        | Tags                |
|-------------------------------------------------------------------------------------------------------------------------------------------------|----------------------|-------------------------------------------------------------|---------------------|
| <a href="https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-32176">msrc.microsoft.com/update-guide/vulnerability/CVE-2026-32176</a> | secure@microsoft.com | <a href="https://msrc.microsoft.com">msrc.microsoft.com</a> | Vendor Advisory     |
| CVE Program record                                                                                                                              | CVE.ORG              | <a href="https://www.cve.org">www.cve.org</a>               | canonical           |
| NVD vulnerability detail                                                                                                                        | NVD                  | <a href="https://nvd.nist.gov">nvd.nist.gov</a>             | canonical, analysis |

No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.

completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

**Free CVE JSON API** [cve.report/api](https://cve.report/api)

**CVE.report and Source URL Uptime Status** [status.cve.report](https://status.cve.report)