Microsoft Zero-Day Vulnerability Patched

TL;DR

Microsoft's July 2025 Patch Tuesday includes a publicly disclosed zero-day (CVE-2025-49719), which is an information disclosure vulnerability in the SQL Server. This flaw could allow an unauthenticated attacker to steal data over the network.

Although not exploited in the wild, it's the type of vulnerability that's easy to abuse and can quietly exfiltrate data from backend databases. Patching is available and should be prioritized.

Microsoft also addressed 136 other flaws, including multiple remote code execution bugs in Office and SharePoint.

Overview

Microsoft released fixes for 137 security issues this month, but CVE-2025-49719 (CVSS 7.5) stands out as the only zero-day. This Microsoft SQL Server zero-day vulnerability was publicly disclosed and affects a wide range of supported versions.

CVE-2025-49719 is caused by improper input validation. A remote, unauthenticated attacker could exploit the flaw to access uninitialized memory over a network. While the data exposed depends on the contents of that memory, it could include sensitive information or credentials.

Impacted Versions

- Microsoft SQL Server 2016 SP2 (GDR) – affected until build 13.0.6460.7
- SQL Server 2016 SP3 Azure Connect Feature Pack – affected until build 13.0.7055.9
- SQL Server 2017 (GDR) – affected until build 14.0.2075.8
- SQL Server 2017 CU31 – affected until build 14.0.3495.9
- SQL Server 2019 (GDR) – affected until build 15.0.2135.5
- SQL Server 2019 CU32 – affected until build 15.0.4435.7
- SQL Server 2022 (GDR) – affected until build 16.0.4200.1
- SQL Server 2022 CU19 – affected until build 16.0.1140.6

The zero-day was discovered internally by a Microsoft researcher but was already public before the company issued a patch. Even though Microsoft rates exploitation as "less likely," patching as soon as possible is highly recommended if you're running SQL Server.

Other Vulnerabilities

Microsoft also fixed 14 critical vulnerabilities, including multiple remote code execution flaws in Microsoft Office and SharePoint. Office bugs are especially dangerous as they can be triggered via document preview alone. Additional updates include AMD side-channel issues, elevation of privilege flaws, and other memory-related vulnerabilities. A full list of vulnerabilities patched in July can be found on Microsoft's advisory page.

Aspire Protects

- Patch – Users should patch CVE-2025-49719 as soon as possible. Please see Microsoft's security advisory for patch guidance.

TTPs to Watch

Initial Access

- Exploit Public-Facing Application [T1190] – If SQL Server is internet-facing or exposed through a vulnerable web application, attackers could use this flaw to retrieve sensitive memory contents.

Collection

- Data from Information Repositories [T1213] – The attacker may retrieve fragments of application or database content stored in memory.

Credential Access

- Unsecured Credentials [T1552] – If memory contains secrets or tokens, these could be harvested and reused.

IoCs

There are no known IoCs associated with the above vulnerability at this time. Aspire is actively monitoring and will notify customers if any are found. For more details on how we can help protect your organization, contact Aspire's Customer Success Management team.

Targeted Industries

Any industry running Microsoft SQL Server is at risk.

- Finance
- Healthcare
- Retail & Manufacturing

Aspire Service Offerings

- **Aspire Managed XDR (MXDR)**
  - Aspire Managed XDR (MXDR) combines next-generation eXtended Detection and Response (XDR) technology, a 24x7 security operations center (SOC), and the expertise of a US-based team of security professionals to identify and respond to threats across a broader attack surface.
  - Building on the existing capabilities of Managed Detection and Response (MDR), Aspire Managed XDR integrates and correlates telemetry from endpoints, network, cloud, email, identity, and more. This advanced platform creates valuable context enabling end-to-end visibility across all threat vectors.
  - Experienced security analysts and incident responders deliver 24x7 threat detection, analysis, and investigations – with both automated and human-led response actions to quickly mitigate cyber attacks.
- **Aspire Incident Response**
  - The ability to respond effectively to data breaches is critical to every organization. When attacks occur, IT leaders need a process that will ultimately maintain business continuity, protect the company reputation, and avoid fines, legal fees, and remediation costs.
  - Aspire offers incident response services to help you prepare for, manage, and recover from data breaches and network attacks. An experienced team uses industry-leading threat intelligence and the most current security technology to quickly respond to attacks, reduce damage, and minimize exposure.

Supporting Documentation

July 2025 Security Updates - Release Notes - Security Update Guide - Microsoft

CVE-2025-49719 - Security Update Guide - Microsoft - Microsoft SQL Server Information Disclosure Vulnerability

Security Update Guide - Microsoft