Microsoft March Patch Tuesday Fixes Two Zero-Day Vulnerabilities

TL;DR

Microsoft's Patch Tuesday addresses 79 vulnerabilities across Windows, SQL Server, .NET, Office, and other Microsoft products, including two zero-day vulnerabilities.

The zero-days affect Microsoft SQL Server (CVE-2026-21262) and .NET (CVE-2026-26127). Neither vulnerability is known to be exploited in the wild yet, but both were publicly disclosed before patches were released.

Organizations should prioritize patching systems running SQL Server and .NET.

Overview

Microsoft released its March 2026 Patch Tuesday security updates, patching 79 vulnerabilities across multiple Microsoft products, including Windows components, Azure services, Office applications, SQL Server, and .NET frameworks.

Among the issues fixed this month are two zero-day vulnerabilities that were known before patches became available. While neither vulnerability has been exploited, public disclosure increases the likelihood that threat actors will begin testing them quickly.

CVE-2026-21262 (CVSS 8.8)

- This zero-day affects Microsoft SQL Server and allows a network-based attacker with valid access to elevate privileges to SQL sysadmin level due to improper access control. If exploited, the attacker could gain SQL sysadmin privileges and take control of the affected SQL Server instance.

CVE-2026-26127 (CVSS 7.5)

- This zero-day impacts .NET and results from an out-of-bounds read condition that allows an attacker to trigger a denial-of-service condition remotely. An attacker could send specially crafted network requests that cause the affected application or service to crash, potentially interrupting critical business applications built on the .NET platform.

Affected Products

- Microsoft SQL Server
- Microsoft .NET and .NET Runtime
- Microsoft Office (including Excel)
- Microsoft SharePoint Server
- Microsoft Windows Components
- Microsoft Azure Services

In addition to the two zero-days, Microsoft addressed 77 additional vulnerabilities across its ecosystem. These include multiple remote code execution vulnerabilities in Microsoft Office, including two flaws (CVE-2026-26110 and CVE-2026-26113) that can be triggered through the Office preview pane, as well as numerous elevation-of-privilege issues affecting Windows components and services. Microsoft also patched a Microsoft Excel information disclosure vulnerability (CVE-2026-26144) that could allow data exfiltration through Microsoft Copilot under certain conditions.

Even though the other vulnerabilities are not zero-days, there are still a large number of privilege escalation issues in this release. Once attackers study the patches, these types of flaws often start showing up in follow-on attacks.

Aspire Protects

- **Patch** - Apply the March 2026 Microsoft security updates for the two zero-day vulnerabilities as soon as possible. See Microsoft's advisories for more information.
    - CVE-2026-21262
    - CVE-2026-26127
    - Please see Microsoft's Security Update Guide for the full list of vulnerabilities addressed in this Emergency Flash Notice.
- Prioritize patching systems running Microsoft SQL Server and .NET
- Monitor SQL Server environments for unusual administrative activity or unexpected privilege changes
- Investigate repeated application crashes affecting .NET-based services

TTPs to Watch

Initial Access

- Exploit Public-Facing Application [T1190] – The attacker may target exposed SQL Server services or vulnerable applications to exploit the SQL Server privilege escalation vulnerability.

Impact

- Endpoint Denial of Service [T1499] – The attacker may send specially crafted requests to a vulnerable .NET service to crash the application and interrupt service availability.

IoCs

There are no known IoCs 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

Microsoft platforms are widely used across enterprise environments. Organizations operating Microsoft infrastructure may be affected, including those in the following sectors:

- Education
- Energy
- Finance
- Healthcare
- Legal
- Manufacturing
- Public Sector
- Retail

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

CVE-2026-21262 - Security Update Guide - Microsoft - SQL Server Elevation of Privilege Vulnerability

CVE-2026-26127 - Security Update Guide - Microsoft - .NET Denial of Service Vulnerability