SharePoint and Public Defender Zero Days Patched by Microsoft

TL;DR

Microsoft released patches for 165 vulnerabilities, including two zero-days.

CVE-2026-32201 (CVSS 6.5) in SharePoint is actively exploited and allows spoofing over the network. CVE-2026-33825 (CVSS 7.8) in Microsoft Defender was publicly disclosed and can give attackers SYSTEM-level access.

Organizations should prioritize patching SharePoint and confirming Defender updates are applied.

Overview

This week, Microsoft addressed 165 vulnerabilities, including two zero-days. The first, CVE-2026-32201 (CVSS 6.5), is a SharePoint Server spoofing vulnerability that is already being exploited in the wild. The second, CVE-2026-33825 (CVSS 7.8), affects Microsoft Defender and was publicly disclosed prior to patching.

Affected Products

- Microsoft SharePoint Server Subscription Edition
- Microsoft SharePoint Server 2019
- Microsoft SharePoint Enterprise Server 2016
- Microsoft Defender (Antimalware Platform versions prior to 4.18.26030.3011)

While Microsoft addressed a large number of additional vulnerabilities, including remote code execution flaws in Office and multiple elevation of privilege issues, this notice focuses on the two zero-days due to active exploitation and the risk of use.

CVE-2026-32201 (CVSS 6.5)

- This is a Microsoft SharePoint Server spoofing vulnerability that is currently being exploited. It is caused by improper input validation and allows an unauthenticated attacker to perform spoofing over the network. If exploited, it can lead to data exposure, phishing/social engineering attacks, and unauthorized changes to content.

CVE-2026-33825 (CVSS 7.8)

- This is a Microsoft Defender elevation of privilege vulnerability. It stems from insufficient access control and allows a local attacker with low privileges to elevate to SYSTEM-level access. If exploited, an attacker can take full control of the system and access sensitive data. They can also modify or disable

protections. The vulnerability was publicly disclosed before patching and a proof-of-concept code has already circulated. Even though exploitation requires local access, the vulnerability becomes more likely to be used when paired with phishing or another initial access method.

Aspire Protects

- **Patch** - Apply April 2026 Microsoft patches immediately. Prioritize the SharePoint vulnerability.
  - CVE-2026-32201
  - CVE-2026-33825
- Verify SharePoint servers are updated to the latest build versions
- Confirm Microsoft Defender platform updates are installed (should update automatically, but check it to be sure)
- Monitor SharePoint activity for unusual content changes or suspicious user interactions
- Watch for signs of phishing or internal spoofing attempts tied to SharePoint
- To view Microsoft's full list of April security updates, including all 165 vulnerabilities, see this link

TTPs to Watch

Initial Access

- Phishing [T1566] – The attacker may use spoofed SharePoint content to trick users into trusting malicious links or files (CVE-2026-32201)

Defense Evasion

- Masquerading [T1036] – The attacker may manipulate trusted SharePoint content to appear legitimate and bypass user suspicion (CVE-2026-32201)

Privilege Escalation

- Exploitation for Privilege Escalation [T1068] – The attacker may exploit a local vulnerability to gain SYSTEM-level access on a host (CVE-2026-33825)

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

Organizations using Microsoft SharePoint Server or Microsoft Defender are at increased risk from these vulnerabilities.

- 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-2026-32201 - Security Update Guide - Microsoft - Microsoft SharePoint Server Spoofing Vulnerability

CVE-2026-33825 - Security Update Guide - Microsoft - Microsoft Defender Elevation of Privilege Vulnerability

April 2026 Security Updates - Release Notes - Security Update Guide - Microsoft