CERT-EU

Security Advisory 2026-009

Critical Vulnerabilities in Microsoft SharePoint

2026-07-22 — v1.1

TLP:CLEAR

History:

- *22/07/2026 — v1.0 – Initial publication*
- *22/07/2026 — v1.1 – Updated to include additional actively exploited vulnerabilities (CVE-2026-32201, CVE-2026-45659, CVE-2026-56164, and CVE-2026-58644)*

Summary

[UPDATED] On 14 July 2026, Microsoft released security updates addressing critical remote code execution (RCE) vulnerabilities in Microsoft SharePoint Server [1]. On 20 July 2026, WatchTowr identified a proof-of-concept exploit code and subsequently observed active exploitation of **CVE-2026-50522** [2], a vulnerability part of an ongoing series of actively exploited flaws [3] affecting on-premise SharePoint Server instances, including **CVE-2026-32201**, **CVE-2026-45659**, **CVE-2026-56164**, and **CVE-2026-58644**.

CERT-EU strongly recommends updating affected servers immediately, rotating credentials for any assets that may have been exposed to the internet, and conducting a compromise assessment.

Technical Details

[UPDATED] The vulnerability **CVE-2026-50522** (CVSS: 9.8) is a critical deserialisation vulnerability in Microsoft SharePoint that allows a remote attacker to execute arbitrary code on affected systems. While Microsoft indicates that exploitation requires some level of authentication [1], recent findings suggest this may not be the case [2, 4].

[NEW] Over the past month, Microsoft also fixed the following vulnerabilities affecting Microsoft SharePoint Server:

- **CVE-2026-32201**: An improper input validation flaw enabling spoofing attacks by an unauthorised user (CVSS: 6.5) [5]. Fixed in April 2026.
- **CVE-2026-45659**: A deserialisation of untrusted data vulnerability allowing authenticated remote code execution (CVSS: 8.8) [6]. Fixed in May 2026.
- **CVE-2026-56164**: Missing authentication for a critical function, allowing unauthenticated privilege escalation (CVSS: 9.8) [7]. Fixed in July 2026.
- **CVE-2026-58644**: A deserialisation vulnerability enabling unauthenticated remote code execution (CVSS: 9.8) [8]. Fixed in July 2026.

Affected Products

[UPDATED] The vulnerability **CVE-2026-50522** affects the following Microsoft SharePoint products. Refer to the respective Microsoft advisories [5–8] for the full list of affected products for the other vulnerabilities.

- Microsoft SharePoint Server Subscription Edition
- Microsoft SharePoint Server 2019
- Microsoft SharePoint Enterprise Server 2016

Recommendations

CERT-EU strongly recommends updating affected servers as soon as possible, rotating credentials for any assets that may have been vulnerable and exposed to the internet, and conducting a compromise assessment to identify potentially affected SharePoint instances.

Given the number of recent critical vulnerabilities affecting SharePoint, organisations should reconsider exposing any Microsoft SharePoint Server directly to the internet.

References

[1] https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-50522

[2] https://www.linkedin.com/posts/watchtowr_exploitation-alert-watchtowr-is-observing-activity-7485278595850940416-LSP8/

[3] https://www.cisa.gov/news-events/alerts/2026/07/14/cisa-urges-sharepoint-hardening-after-new-exploitations

[4] https://x.com/DefusedCyber/status/2079128402855116858

[5] https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-32201

[6] https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-45659

[7] https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-56164

[8] https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-58644