CERT-EU

Security Advisory 2026-004

Critical Vulnerability in SharePoint Exploited

2026-03-25 — v1.0

TLP:CLEAR

History:

- *25/03/2026 — v1.0 – Initial publication*

Summary

On 17 March 2026, Microsoft updated one of its January 2026 security advisories related to a remote code execution vulnerability in Microsoft SharePoint [1]. Specifically, Microsoft raised the CVSS score and changed the FAQ section to indicate that the vulnerability could be exploited by an unauthenticated attacker. This vulnerability was added in the CISA's Known Exploited Vulnerabilities (KEV) catalogue on 18 March 2026 [2].

Additionally, three further RCE flaws affecting Microsoft SharePoint were addressed in the March 2026 release [3,4,5].

CERT-EU strongly recommends updating SharePoint servers as soon as possible, prioritising internet-facing assets. CERT-EU also encourages IT administrators to take necessary remediation actions.

Technical Details

The vulnerability **CVE-2026-20963**, with a CVSS score of 9.8, is an unauthenticated remote code execution vulnerability in Microsoft SharePoint. The flaw is due to deserialisation of untrusted data [1].

Affected Products

The vulnerability affects Microsoft SharePoint Server Subscription Edition, Microsoft SharePoint Server 2019 and Microsoft SharePoint Enterprise Server 2016.

Additional information is available in the vendor's advisories [1,3,4,5].

Recommendations

CERT-EU strongly recommends updating SharePoint servers as soon as possible, prioritising internet-facing assets.

While no additional information is available and considering the Sharepoint exploitation campaign in 2025 for which we have issued a security advisory 2025-027 [9], CERT-EU recommends IT administrators, as a precautionary measure, to apply the same remediation steps once the concerned servers are up-to-date, namely:

- Enable the Antimalware Scan Interface (AMSI) in enable Full Mode [7].
- Deploy an EDR solution.
- Rotate SharePoint Server ASP.NET machine keys [8] and restart IIS using `iisreset.exe`.

It is also advised to conduct a compromise assessment on internet-facing assets.

References

[1] https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-20963

[2] https://cybersecuritynews.com/microsoft-sharepoint-vulnerability-exploited/

[3] https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-26106

[4] https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-26113

[5] https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-26114

[6] https://www.microsoft.com/en-us/security/blog/2025/07/22/disrupting-active-exploitation-of-on-premises-sharepoint-vulnerabilities/

[7] https://learn.microsoft.com/en-us/sharepoint/security-for-sharepoint-server/configure-amsi-integration#configure-amsi-via-user-interface

[8] https://learn.microsoft.com/en-us/sharepoint/security-for-sharepoint-server/improved-asp-net-view-state-security-key-management

[9] https://www.cert.europa.eu/publications/security-advisories/2025-027/