Microsoft SharePoint Server Multiple Vulnerabilities (Actively Exploited)

Severity Level: Critical

Components Affected

- Microsoft SharePoint Server Subscription Edition
- Microsoft SharePoint Server 2019 (end of support since 14 July 2026)
- Microsoft SharePoint Enterprise Server 2016 (end of support since 14 July 2026)
- Microsoft Project Server 2013 SP1 and Office Web Apps 2013 SP1

SharePoint Online (Microsoft 365) is not affected.

Overview

Multiple vulnerabilities have been identified in on-premises Microsoft SharePoint Server. A remote, unauthenticated attacker could chain two of these to impersonate any user, including a site administrator, and execute arbitrary code on the affected server without credentials or user interaction. Proof-of-concept exploit code is publicly available and already in use in attacks. A separate SharePoint remote code execution flaw is confirmed by CISA as being exploited in ransomware campaigns.

Description

A technical write-up and working proof-of-concept for CVE-2026-55040 were published on 11 August 2026. Within roughly twenty-four hours, the exploit was observed in use against internet-exposed SharePoint honeypots. Details of the most significant vulnerabilities are as follows:

- **CVE-2026-55040 (CVSS 9.1) –** Authentication bypass in the JWT validation pipeline, allowing an unauthenticated attacker to impersonate a chosen user and disclose files or modify data. Assessed as automatable with total technical impact.
- **CVE-2026-63520 (CVSS 8.1) –** Unsafe .NET type instantiation in Business Connectivity Services, executing attacker code as the site service account. Chained with CVE-2026-55040, this yields unauthenticated remote code execution.
- **CVE-2026-45659 –** Deserialization of untrusted data allowing a low-privileged attacker to execute code in low-complexity, repeatable attacks. In the CISA Known Exploited Vulnerabilities Catalog since 1 July 2026 and confirmed on 11 August 2026 as used in ransomware campaigns.
- **CVE-2026-65665, CVE-2026-64921, CVE-2026-62827 –** Three further SharePoint vulnerabilities rated Critical, among approximately twenty fixed in the August 2026 release.

Shadowserver tracks over 8,500 SharePoint servers exposed to the internet. CISA has catalogued fourteen actively exploited SharePoint vulnerabilities since November 2021, eight later used in ransomware attacks.

Impact

- Remote Code Execution
- Authentication Bypass / User Impersonation
- Elevation of Privilege
- Information Disclosure and Data Manipulation
- Ransomware Deployment

Solution/ Workarounds

Apply fixes issued by the vendor:

- July 2026 update, which breaks the exploit chain Subscription Edition KB5002882 (16.0.19725.20434), SharePoint Server 2019 KB5002883 (16.0.10417.20175), SharePoint Enterprise Server 2016 KB5002891 (16.0.5561.1001).
- August 2026 cumulative update, released 11 August 2026, addressing CVE-2026-63520 and approximately twenty further flaws. Apply the full update rather than selecting individual CVEs.
- May 2026 update addressing CVE-2026-45659.
- Verify patch status by build number, not by patch management console reporting alone.

Recommended hardening and monitoring measures:

- Remove direct internet exposure where there is no documented business need and block external access to Central Administration; where exposure is unavoidable, place the server behind a Layer 7 reverse proxy or equivalent control.
- Enable AMSI integration for SharePoint web applications and confirm endpoint protection is healthy on all SharePoint servers.
- Forward IIS access logs, Windows Security event logs with command line auditing, and endpoint telemetry to the organisation's monitoring platform.

Patching alone is not sufficient for a server that was internet-exposed and unpatched. Earlier campaigns stole IIS machine keys, which let an attacker forge authentication material and retain access after the flaw is closed. Hunt for web shells and key-harvesting artefacts before rotating machine keys; signs of compromise call for full incident response.
SharePoint Server 2016 and 2019 reached end of support on 14 July 2026 and will receive no new security updates. Migration should be treated as an urgent risk-reduction measure.

Reference

- https://nvd.nist.gov/vuln/detail/CVE-2026-55040
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-55040
- https://learn.microsoft.com/en-us/officeupdates/sharepoint-updates
- https://www.cisa.gov/known-exploited-vulnerabilities-catalog

Disclaimer

The information provided herein is on an "as is" basis, without warranty of any kind.