Microsoft SharePoint Server Deserialization Remote Code Execution Vulnerability

Severity Level: HIGH

Components Affected

- Microsoft SharePoint Server 2019 versions earlier than 16.0.10417.20128
- Microsoft SharePoint Enterprise Server 2016 versions earlier than 16.0.5552.1002
- Microsoft SharePoint Server Subscription Edition versions earlier than 16.0.19725.20280
- On-premises SharePoint Server deployments running affected x64-based systems

Overview

A high-severity remote code execution vulnerability has been identified in Microsoft SharePoint Server. The vulnerability exists due to deserialization of untrusted data and may allow an authorized attacker to execute code over a network on affected SharePoint Server systems.

CISA has added CVE-2026-45659 to the Known Exploited Vulnerabilities catalog following evidence of active exploitation. Organizations using affected SharePoint Server versions are strongly advised to apply Microsoft security updates urgently and review exposed SharePoint environments for signs of compromise.

Description

CVE-2026-45659 is a deserialization of untrusted data vulnerability in Microsoft Office SharePoint. The issue is categorized under CWE-502: Deserialization of Untrusted Data. The vulnerability has a CVSS v3.1 base score of 8.8 and is rated High.

Successful exploitation requires an authenticated, low-privileged attacker with network access to the SharePoint Server. The CVSS vector indicates low attack complexity, low privileges required, and no user interaction required. If exploited successfully, an attacker may be able to execute code remotely on the affected server.

Depending on the configuration and privileges available on the compromised SharePoint server, exploitation may allow the attacker to execute malicious commands, access sensitive information, modify SharePoint content, deploy additional payloads, or use the server as a pivot point for further internal network activity.

Impact

- Remote Code Execution
- Unauthorized Code Execution on SharePoint Server
- Sensitive Information Disclosure
- Potential Server Compromise
- Potential Lateral Movement within the Network
- Service Disruption

Solution/ Workarounds

- Apply the relevant Microsoft SharePoint Server security updates immediately.
- Upgrade Microsoft SharePoint Enterprise Server 2016 to build 16.0.5552.1002 or later.
- Upgrade Microsoft SharePoint Server 2019 to build 16.0.10417.20128 or later.
- Prioritize remediation for internet-facing or externally accessible SharePoint servers.
- Restrict SharePoint administrative and user access to trusted networks where possible.
- Review SharePoint, IIS, Windows Event, EDR, and proxy logs for suspicious authenticated access, unusual file uploads, unexpected child processes, web shells, or new administrative accounts.
- Enforce least privilege for SharePoint users and review Site Member, Site Owner, and administrative permissions.
- Ensure reliable backups are available and verify restoration procedures for critical SharePoint content and configuration databases.
- If compromise is suspected, isolate the affected server, preserve forensic evidence, rotate credentials, and perform incident response activities before returning the system to production.

Reference

- https://nvd.nist.gov/vuln/detail/CVE-2026-45659
- https://www.cisa.gov/news-events/alerts/2026/07/01/cisa-adds-one-known-exploited-vulnerability-catalog
- https://www.cisa.gov/known-exploited-vulnerabilities-catalog?field_cve=CVE-2026-45659
- https://cyberveille.esante.gouv.fr/alertes/microsoft-cve-2026-45659-2026-05-27

Disclaimer

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