WHITE PAPER

CYTEX™
AI-Powered Resilience Command Center

Microsoft SharePoint Server Vulnerability
Allows Authenticated Remote Code Execution

hello@cytex.io | https://cytex.io

SharePoint Server Authenticated RCE via Untrusted Deserialization

Technical analysis of the SharePoint Server deserialization vulnerability allowing remote code execution from a low-privilege Site Member account, with affected versions and mitigation guidance.

What Happened

Microsoft has disclosed CVE-2026-45659, a critical remote code execution vulnerability in SharePoint Server caused by deserialization of untrusted data within Microsoft Office SharePoint. The flaw allows an authenticated attacker to execute arbitrary code on the server over the network. The minimum privilege required to exploit the vulnerability is Site Member, which is the standard user role granted to any account with collaborative access to a SharePoint site. No administrator role, no elevated privileges, and no specialized exploitation conditions are required.

The vulnerability was discovered and reported by a researcher identified as MEOW. Microsoft has released security updates for all affected SharePoint Server versions.

For most enterprise SharePoint deployments, the Site Member role is held by a substantial fraction of the user population. Internal users with routine collaboration access, contractors with project-scoped membership, and external partners invited to shared sites all typically hold this role or higher. The exploitation precondition is met by default in most environments.

Vulnerability Profile

Attribute	Detail
CVE	CVE-2026-45659
Class	Remote code execution via deserialization of untrusted data
Affected component	Microsoft Office SharePoint
CVSS 3.1 base score	8.8 (High)
CVSS vector summary	Network attack vector, low complexity, low privileges, no user interaction, scope unchanged, high impact on confidentiality, integrity, and availability
Required privilege	Site Member (PR:L) or higher
User interaction required	None

Attribute	Detail
Attack vector	Network
Affected versions	SharePoint Server Subscription Edition; SharePoint Server 2019; SharePoint Enterprise Server 2016
Patch status	Updates released by Microsoft for all affected versions
Discloser	Researcher MEOW

How the Vulnerability Works

The defect is a deserialization of untrusted data flaw inside Microsoft Office SharePoint. Deserialization vulnerabilities arise when an application converts serialized input back into in-memory objects without sufficient validation of the input source or the resulting object types. An attacker who can supply serialized content to the vulnerable code path can craft input that, during deserialization, instantiates objects whose construction or method invocation produces unintended behavior, including arbitrary code execution in the context of the server process.

In the case of CVE-2026-45659, the SharePoint Server processes serialized data submitted through authenticated user-accessible interfaces without sufficient guardrails on the types and content being deserialized. An authenticated attacker holding the Site Member role can submit crafted serialized payloads that trigger code execution on the SharePoint Server itself. The code runs with the privileges of the SharePoint service account.

The architectural pattern this exploits is consistent with the broader class of .NET deserialization vulnerabilities that have appeared repeatedly in SharePoint and other Microsoft server products over the past decade. The exploitation primitive is well understood by the offensive research community, and public gadget chains for .NET deserialization are extensively documented. Once a deserialization sink is reachable by an authenticated user, weaponization is straightforward.

Why the Privilege Threshold Matters

The PR:L (low privilege) designation in the CVSS vector is the operationally consequential detail. SharePoint's permission model defines Site Member as a default role for users contributing to a site, distinct from Site Visitor (read-only) and Site Owner (administrative). In a typical enterprise environment:

- All employees with access to a collaboration site hold Site Member or higher by default
- Contractors granted project access are routinely added at the Site Member level
- External users invited through guest access patterns are often added at the Site Member level

- Service accounts and automation identities frequently hold Site Member roles for integration purposes

The vulnerability therefore does not require an attacker to compromise a privileged account or to escalate from a foothold. Any user account with collaboration access can exploit the vulnerability directly. The realistic threat scenarios include:

- An insider with routine collaboration access escalating to server compromise
- An external attacker who has phished or otherwise obtained a single internal user's credentials
- An external partner or contractor account abusing the relationship
- A compromised service account integrated with SharePoint pivoting to full server control
- Lateral movement from a single compromised endpoint into the SharePoint infrastructure layer

The compromise of a SharePoint Server has substantial downstream consequences. SharePoint commonly stores intellectual property, contracts, HR records, financial documents, and internal communications. The service account context in which exploitation succeeds typically has access to backend SQL databases, Active Directory integration paths, and adjacent Microsoft 365 infrastructure.

Affected Versions

The vulnerability affects on-premises SharePoint Server deployments across the following versions:

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

Microsoft has released security updates for each affected version through standard Patch Tuesday delivery channels. Organizations should refer to the official Microsoft Security Response Center advisory for CVE-2026-45659 for the specific update KB numbers and download paths corresponding to each version.

SharePoint Online (the Microsoft 365 hosted service) is not specifically named in the vulnerability disclosure. Customers on the hosted service inherit Microsoft's service-layer remediation timeline directly and do not need to apply patches manually.

Indicators and Detection Signals

The vulnerability does not produce a single deterministic IOC, since exploitation uses authenticated user-accessible interfaces and the malicious payload appears as serialized content rather than as a distinct malware family. Detection is behavioral and log-driven, focused on the deserialization sink and the post-exploitation behaviors that follow.

Pre-exploitation signals:

- Unusual POST requests to SharePoint endpoints carrying serialized .NET payloads from low-privilege user accounts
- Requests containing patterns associated with public .NET deserialization gadget chains (TypeConfuseDelegate, ObjectDataProvider, and similar markers, where deep packet inspection is in scope)
- Authenticated requests to SharePoint endpoints from accounts that have no historical interaction with the affected functionality
- Spikes in 500-class errors on SharePoint application servers correlated with specific user accounts, which may indicate exploitation attempts before successful weaponization

Post-exploitation signals on the SharePoint Server:

- Unexpected child processes spawned by w3wp.exe (the IIS worker process hosting SharePoint), particularly cmd.exe, powershell.exe, wscript.exe, cscript.exe, or other command interpreters
- PowerShell invocations from the SharePoint application pool service account with encoded command lines, network connections, or download-and-execute patterns
- File creation in SharePoint installation directories or temporary paths by the application pool identity, with file types or paths inconsistent with normal SharePoint operation
- Outbound network connections from the SharePoint server to destinations outside the configured integration scope, particularly to file-sharing services, paste sites, or unknown IP addresses
- New scheduled tasks, services, or persistence mechanisms created on the SharePoint server immediately following authenticated activity from a low-privilege account
- Modifications to the SharePoint configuration, including new web parts, custom solutions, or feature activations that do not correspond to administrative change records

Authentication and authorization signals:

- Unusual login patterns to Site Member accounts immediately preceding SharePoint exploitation activity, including logins from new geographic locations or unfamiliar IP ranges
- Token theft indicators on endpoints belonging to Site Member account holders, since stolen credentials are a likely amplifier for this vulnerability

Defensive Actions

Apply the patch immediately across all affected SharePoint Server installations. Microsoft has released updates for all three affected versions. Patching is the only definitive remediation. Out-of-cycle deployment is warranted given the low privilege threshold and the deserialization class history of being rapidly weaponized.

Audit Site Member and higher role assignments. Identify which accounts hold Site Member access across all SharePoint sites in the environment. Disable or downgrade accounts that no longer require collaboration access. Pay particular attention to dormant accounts, departed employees, expired contractor relationships, and external guest accounts.

Apply step-up authentication to SharePoint access where operationally feasible. Multi-factor authentication on every SharePoint authentication event raises the cost of credential-based exploitation. Conditional access policies that restrict SharePoint access to managed devices or compliant network locations further reduce the population of accounts an external attacker can leverage.

Instrument the SharePoint application pool for child-process and outbound-connection monitoring. EDR or Sysmon coverage on SharePoint application servers should flag any process spawned by w3wp.exe outside the documented SharePoint process tree, and any outbound connection from the application pool identity to non-allowlisted destinations. These signals catch post-exploitation behavior even if the initial deserialization request is missed.

Audit SharePoint logs for the exposure window. Review SharePoint Unified Logging Service (ULS) logs, IIS access logs, and Windows event logs on SharePoint application servers for anomalous activity during the window between SharePoint version release and patch application. Focus on authenticated POST requests with abnormal payload sizes, requests resulting in server-side errors followed by successful subsequent activity, and any indication of the post-exploitation behavioral signals above.

Treat SharePoint Server as a high-value asset under the standard hardening posture. Beyond this specific CVE, the broader hardening recommendations for SharePoint deployments apply: restrict the SharePoint service account to least-privilege configurations, segment SharePoint servers on the network, enable comprehensive logging, and integrate SharePoint authentication events with SIEM correlation.

Plan for the next deserialization disclosure. Deserialization vulnerabilities in SharePoint have appeared repeatedly across multiple major releases over the past decade and have been

weaponized by both criminal and state-aligned actors within days of disclosure. The recurrence pattern is structural rather than incidental. Defensive programs should treat the deserialization sink class as a category-level risk and maintain the compensating controls above as standing capabilities rather than incident-driven deployments.

Sources

- Microsoft Security Response Center advisory for CVE-2026-45659
- Microsoft SharePoint Server security update documentation
- Discovery and reporting credited to researcher MEOW