Hive Pro

Threat Level

Red

Hiveforce Labs

THREAT ADVISORY

VULNERABILITY REPORT

CVE-2026-45659: SharePoint's Open Door, Patch It Now

Date of Publication	Admiralty Code	TA Number
July 03, 2026	A1	TA2026186

Summary

First Seen: May 2026
Affected Products: Microsoft SharePoint Server Subscription Edition, Microsoft SharePoint Server 2019, Microsoft SharePoint Enterprise Server 2016
Impact: CVE-2026-45659 is a high-severity remote code execution flaw in Microsoft SharePoint Server, rooted in the insecure deserialization of untrusted data (CWE-502). An attacker who has already authenticated to a targeted server, needing only standard Site Member permissions, can send a crafted payload over the network and run arbitrary code on the underlying SharePoint instance without any user interaction. The weakness affects on-premises deployments, specifically SharePoint Server Subscription Edition, SharePoint Server 2019, and SharePoint Enterprise Server 2016. Microsoft shipped fixes in late May 2026 as an out-of-band correction after the CVE was inadvertently omitted from the May 2026 Security Updates. The vulnerability is now confirmed to be actively exploited, making patching crucial.

CVE

CVE	NAME	AFFECTED PRODUCT	ZERO-DAY	CISA KEV	PATCH
CVE-2026-45659	Microsoft SharePoint Server Deserialization of Untrusted Data Vulnerability	Microsoft SharePoint Server	✗	✓	✓

Vulnerability Details

#1

SharePoint's habit of trusting the data it receives has once again turned into a liability. CVE-2026-45659 is classified under CWE-502, Deserialization of Untrusted Data, meaning the server reconstructs attacker-controlled objects without validating them first, a flaw class that reliably translates into code execution when abused. A specially crafted serialized payload submitted to a vulnerable endpoint is deserialized in a way that lets the attacker's data drive the execution flow, resulting in arbitrary code running in the context of the SharePoint application. Microsoft notes that the attack complexity is low because an adversary does not need deep prior knowledge of the system and can reliably reproduce success with the payload against the affected component.

#2

The attack is carried out over the network and is remotely reachable from the internet, but it is not unauthenticated; an attacker must first hold valid credentials with at least Site Member permissions before triggering the flaw. This authentication requirement is the only meaningful hurdle; no elevated or administrative rights are required, and no user interaction is involved once the attacker is logged in. The vulnerability affects on-premises SharePoint installations, specifically SharePoint Server Subscription Edition, SharePoint Server 2019, and SharePoint Enterprise Server 2016.

#3

Microsoft addressed the issue through the May 2026 update cycle, though the CVE identifier was inadvertently omitted from the published May 2026 Security Updates and later documented separately; customers who had already applied the May 2026 updates were told no further action was needed. The fixes correspond to SharePoint Server Subscription Edition build 16.0.19725.20280, SharePoint Server 2019 build 16.0.10417.20128, and SharePoint Enterprise Server 2016 build 16.0.5552.1002. The vulnerability is now confirmed to be actively exploited, making patching crucial. Users who have already installed the May 2026 updates do not need to take any further action.

Vulnerability

CVE ID	AFFECTED PRODUCTS	AFFECTED CPE	CWE ID
CVE-2026-45659	Microsoft SharePoint Server Subscription Edition, SharePoint Server 2019, SharePoint Enterprise Server 2016	cpe:2.3:a:microsoft:sharepoint_server:2019:*:*:*:*:*:*:*, cpe:2.3:a:microsoft:sharepoint_server:2016:*:*:*:*:enterprise:*:*:*, cpe:2.3:a:microsoft:sharepoint_server:-:*:*:*:*:subscription:*:*:*	CWE-502

Recommendations

Apply Microsoft's Security Updates Immediately: Install the May 2026 updates that remediate CVE-2026-45659 on every affected on-premises SharePoint server without delay. The fixed builds are SharePoint Server Subscription Edition 16.0.19725.20280, SharePoint Server 2019 16.0.10417.20128, and SharePoint Enterprise Server 2016 16.0.5552.1002. Because the flaw is under active exploitation, patching is the single most effective action available.

Verify Patch Coverage Across the Estate: Confirm that the deployed build numbers match or exceed the fixed versions on each server, since the CVE was originally omitted from the May 2026 Security Updates and administrators may wrongly assume they are protected. Reconcile your inventory against the vendor advisory to ensure no on-premises instance, including secondary farms and disaster-recovery nodes, was missed.

Tighten SharePoint Account Access: Exploitation only requires an authenticated user with Site Member permissions, so review and prune user accounts, enforce strong authentication, and remove unnecessary or stale low-privilege access. Prioritize multi-factor authentication and least-privilege principles to shrink the pool of credentials an attacker could leverage to reach the vulnerable endpoint.

Limit Internet Exposure and Segment Access: Where patching cannot be completed immediately, restrict inbound access to SharePoint servers, place them behind VPN or zero-trust controls, and segment them from the broader network to reduce the attack surface. With more than 10,000 SharePoint servers observed exposed online, minimizing direct internet reachability materially lowers risk, and CISA advises following BOD 26-04 guidance for cloud services or discontinuing use of the product where mitigations are unavailable.

Potential MITRE ATT&CK TTPs

Tactic	Technique	Sub-technique
Initial Access	T1190: Exploit Public-Facing Application	
Execution	T1059: Command and Scripting Interpreter	
Resource Development	T1588: Obtain Capabilities	T1588.006: Vulnerabilities

Patch Link

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

References

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

What Next?

At **Hive Pro**, it is our mission to detect the most likely threats to your organization and to help you prevent them from happening.

Book a Demo of **HivePro**.

REPORT GENERATED ON

July 03, 2026 • 7:30 AM

More at www.hivepro.com