Smarttech
YOUR 24/7 SECURITY PARTNER

Microsoft SharePoint Server Vulnerability Actively Exploited

Document ID	SMA-Threat Report
Document status	ISSUED
Issue Number	108
Authors	Dorin Constantin Banu < constantin.banu@smarttech247.com >
Verified by	Alin Curcan < alin.curcan@smarttech247.com >
Last modified	2026-07-02
Issue Date	2026-07-02

Threat Reports are reports created by Smarttech247 based on high and critical severity vulnerabilities that may have a high potential to be exploited in the wild i.e. vulnerabilities that are present in most used products by companies and do not have an auto-update option or they are usually not automatically updated in case that could lead to some service disruption. This report is usually created as soon as the vulnerability is released, therefore we strongly recommend that the information is reviewed, tests are performed and patches are applied before the first proof-of-concept is released.
Even though certain vulnerabilities may not have an active exploit in the wild at the time that we report on them, we take into consideration the wider risk and the impact it could have on systems, should an exploit like that be available after a while. Our duty is to report them on time and we recommend enterprises that, in order to keep critical business systems protected, they should consider, on average, ten working days to check whether or not the new vulnerability affects them, and if so, to implement actions in order to remove the risk.

Overview

A high severity vulnerability in Microsoft SharePoint Server is being actively exploited in the wild. Tracked as CVE-2026-45659, this flaw stems from the deserialization of untrusted data. The issue was addressed by Microsoft in May 2026 Patch Tuesday for SharePoint Server Subscription Edition, SharePoint Server 2019, and SharePoint Enterprise Server 2016. The Cybersecurity and Infrastructure Security Agency added this vulnerability to its Known Exploited Vulnerabilities catalog. Federal Civilian Executive Branch agencies are advised to apply the fixes by July 4, 2026.

Risk

Government:

- Large and medium government entities: **High**
- Small government entities: **High**

Businesses:

- Large and medium business entities: **High**
- Small business entities: **High**

Technical summary

More details related to this vulnerability are as follows:

CVE ID	Description
CVE-2026-45659 **CVSS Base Score: 8.8**	Microsoft SharePoint Server contains a deserialization of untrusted data vulnerability which allows an authorized attacker to execute code over a network. Any authenticated attacker could trigger the vulnerability, and that it does not require admin or other elevated privileges. In a network-based attack, an authenticated attacker with a minimum of Site Member permissions (PR:L) could leverage it to execute code remotely on the SharePoint Server.

It's currently not known how the vulnerability is being exploited, who is behind the activity, and what the end goals of these efforts are.

Microsoft also uncovered last month two unrelated attackers operating simultaneously within the same network, while adopting deliberate techniques to establish persistent access and complicate incident response efforts.

One set of attacks has been attributed to Storm-2603, a threat actor known for deploying Warlock ransomware often by exploiting known vulnerabilities in on-premises SharePoint servers since mid-2025. Initial access was likely attempted through a separate vulnerability, with requests for files like win.ini and web.config, indicating probing for local file inclusion. Evidence points to it being CVE-2025-11371 (CVSS score: 9.1), a critical flaw impacting Gladinet Triofox. Upon gaining initial access, the threat actor is said to have deployed tools like Velociraptor to blend malicious activity with trusted administrative behavior, as well as established multiple remote access channels through Cloudflare tunneling, Zoho Assist, and Secure Shell (SSH) connections configured through Visual Studio Code. The attack also escalated privileges by creating new local and domain administrator accounts, while a vulnerable driver ("NSecKrnl.sys") acted as a conduit for tampering with endpoint security protections to help reduce their visibility.

The second attack co-existing in the same environment was using DLL side-loading and custom backdoors, thereby making attribution more challenging. The attackers had moved laterally beyond the first network and into a second organization, which confirmed they had been compromised by the same ransomware activity attributed to Storm-2603.

Together, these overlapping activity streams enabled sustained access while masking the full scope of the intrusion. The blend of known ransomware tactics and hidden techniques allowed the threat actors to establish deep and lasting access.

Affected Products

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

Recommendations

Smarttech247 team recommend the following actions to be taken:

- Apply appropriate patches or appropriate mitigations provided by Microsoft to vulnerable systems immediately after appropriate testing. (**M1051: Update Software**)
    - **Safeguard 7.1: Establish and Maintain a Vulnerability Management Process**: Establish and maintain a documented vulnerability management process for enterprise assets. Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.

    - **Safeguard 7.4: Perform Automated Application Patch Management:** Perform application updates on enterprise assets through automated patch management on a monthly, or more frequent, basis.

- Apply the Principle of Least Privilege to all systems and services, and run all software as a non-privileged user (one without administrative rights) to diminish the effects of a successful attack. (**M1026: Privileged Account Management**)
    - **Safeguard 4.7: Manage Default Accounts on Enterprise Assets and Software:** Manage default accounts on enterprise assets and software, such as root, administrator, and other pre-configured vendor accounts. Example implementations can include: disabling default accounts or making them unusable.
    - **Safeguard 5.4: Restrict Administrator Privileges to Dedicated Administrator Accounts:** Restrict administrator privileges to dedicated administrator accounts on enterprise assets. Conduct general computing activities, such as internet browsing, email, and productivity suite use, from the user's primary, non-privileged account.

- Remind all users not to visit untrusted websites or follow links/open files provided by unknown or untrusted sources. (**M1017: User Training**)
    - **Safeguard 14.1: Establish and Maintain a Security Awareness Program:** Establish and maintain a security awareness program. The purpose of a security awareness program is to educate the enterprise's workforce on how to interact with enterprise assets and data in a secure manner. Conduct training at hire and, at a minimum, annually. Review and update content annually, or when significant enterprise changes occur that could impact this Safeguard.
    - **Safeguard 14.2: Train Workforce Members to Recognize Social Engineering Attacks:** Train workforce members to recognize social engineering attacks, such as phishing, pre-texting, and tailgating.

- Use capabilities to prevent suspicious behavior patterns from occurring on endpoint systems. This could include suspicious process, file, API call, etc. behavior. (**M1040 : Behavior Prevention on Endpoint**)
    - **Safeguard 13.2 : Deploy a Host-Based Intrusion Detection Solution**: Deploy a host-based intrusion detection solution on enterprise assets, where appropriate and/or supported.
    - **Safeguard 13.7 : Deploy a Host-Based Intrusion Prevention Solution:** Deploy a host-based intrusion prevention solution on enterprise assets, where appropriate and/or supported. Example implementations include use of an Endpoint Detection and Response (EDR) client or host-based IPS agent.

References

https://thehackernews.com/2026/07/sharepoint-rce-cve-2026-45659-added-to.html
https://www.microsoft.com/en-us/security/blog/2026/06/22/one-intrusion-two-cyberattackers-uncovering-parallel-threat-activity/
https://www.cisa.gov/news-events/alerts/2026/07/01/cisa-adds-one-known-exploited-vulnerability-catalog
https://www.cve.org/CVERecord?id=CVE-2026-45659

CVE

CVE-2026-45659

Smarttech
YOUR 24/7 SECURITY PARTNER

www.smarttech247.com