CYBER ADVISORY

TLP:CLEAR
20 July 2025

Microsoft SharePoint Zero-Day RCE Vulnerability

SharePoint | RCE | PoC | ToolShell

The California Cybersecurity Integration Center (Cal-CSIC) has identified a critical zero-day vulnerability affecting on-premise Microsoft SharePoint servers. CVE-2025-53770, with a CVSS 3.1 score of 9.8, allows a remote attacker to execute remote code execution (RCE) and gain remote control over vulnerable on-premise SharePoint systems without authentication.[1,2] This vulnerability, also known as ToolShell, appears to be a variant of a previous vulnerability released in May 2025, CVE-2025-49706.[3] There is currently no patch available for this exploitation.

Recommendations and Mitigations: Enable AMSI integration (enabled by default since Sep 2023 updates) and deploy Defender AV on all SharePoint servers; consider offline isolation if AMSI can't be deployed.

Additionally, the Cal-CSIC recommends following the guidance from Microsoft's mitigation efforts.

Defender Signatures:	Exploit:Script/SuspSignoutReq.A
	Trojan:Win32/HijackSharePointServer.A

The Cal-CSIC is currently assessing agencies that may be affected and is making direct notifications. We will continue to share updates as the situation develops. If you need assistance identifying this vulnerability or believe you may be impacted, please reach out, CalCSIC@caloes.ca.gov.

Organization, Source, Reference, and Dissemination Information

Organization Description	California Government Code § 8586.5 established the California Cybersecurity Integration Center (Cal-CSIC) as the central organizing hub of state government's cybersecurity activities, including information sharing, intelligence analysis, incident response, and overarching cybersecurity strategy. The Cal-CSIC is responsible for reducing the likelihood and severity of cyber incidents that could damage California's economy, critical infrastructure, and public or private sector networks in our state.
Customer Feedback	If you need further information about this issue, contact the Cal-CSIC at our email address CalCSIC@caloes.ca.gov or by telephone at (833) REPORT1.
Source Summary Statement	This report was compiled from a variety of sources, predominately open-source reporting.
Handling Caveats	**Traffic Light Protocol (TLP):** Recipients may share TLP:CLEAR information with the world; there is no limit on disclosure. Subject to standard copyright rules, TLP:CLEAR information may be shared without restriction.

[1] National Vulnerability Database; "CVE-2025-53770 Detail" https://nvd.nist.gov/vuln/detail/CVE-2025-53770; accessed 20 July 2025
[2] Microsoft; "Customer Guidance for SharePoint Vulnerability CVE-2025-53770" https://msrc.microsoft.com/blog/2025/07/customer-guidance-for-sharepoint-vulnerability-cve-2025-53770/; accessed 20 July 2025
[3] Eye Research; "ToolShell Mass Exploitation (CVE-2025-53770)" https://research.eye.security/sharepoint-under-siege/; accessed 20 July 2025