An official website of the United States government Here’s how you know

FREE CYBER SERVICES

SECURE BY DESIGN

SECURE OUR WORLD

SHIELDS UP

REPORT A CYBER ISSUE

America’s Cyber Defense Agency

NATIONAL COORDINATOR FOR CRITICAL INFRASTRUCTURE SECURITY AND RESILIENCE

Search

Topics

Spotlight

Resources & Tools

News & Events

Careers

About

ALERT

UPDATE: Microsoft Releases Guidance on Exploitation of SharePoint Vulnerabilities

Last Revised: July 22, 2025

Update (07/22/2025): This Alert was updated to reflect newly released information <https://www.microsoft.com/en-us/security/blog/2025/07/22/disrupting-active-exploitation-of-on-premises-sharepoint-vulnerabilities/> from Microsoft, and to correct the actively exploited Common Vulnerabilities and Exposures (CVEs), which have been confirmed as CVE-2025-49706 <https://nvd.nist.gov/vuln/detail/cve-2025-49706>, a network spoofing vulnerability, and CVE-2025-49704 <https://nvd.nist.gov/vuln/detail/cve-2025-49704>, a remote code execution (RCE) vulnerability.

CISA is aware of active exploitation of a spoofing and RCE vulnerability chain involving CVE-2025-49706 <https://nvd.nist.gov/vuln/detail/cve-2025-49706> and CVE-2025-49704 <https://nvd.nist.gov/vuln/detail/cve-2025-49704>, enabling unauthorized access to on-premise SharePoint servers. While the scope and impact continue to be assessed, the chain, publicly reported as "ToolShell," provides unauthenticated access to systems and authenticated access through network spoofing, respectively, and enables malicious actors to fully access SharePoint content, including file systems and internal configurations, and execute code over the network.

While not actively exploited, Microsoft has identified the following new CVEs that pose a potential risk:

CVE-2025- <https://nvd.nist.gov/vuln/detail/cve-2025-53771>53771 <https://nvd.nist.gov/vuln/detail/cve-2025-53771> is a patch bypass for CVE-2025-49706.
CVE-2025- <https://nvd.nist.gov/vuln/detail/cve-2025-53770>53770 <https://nvd.nist.gov/vuln/detail/cve-2025-53770> is a patch bypass for CVE-2025-49704.

CISA recommends the following actions to reduce the risks associated with the RCE compromise:

- Apply the necessary security updates released by Microsoft <https://www.microsoft.com/en-us/security/blog/2025/07/22/disrupting-active-exploitation-of-on-premises-sharepoint-vulnerabilities/>.

- Configure Antimalware Scan Interface (AMSI) <https://learn.microsoft.com/en-us/windows/win32/amsi/antimalware-scan-interface-portal> in SharePoint as indicated by Microsoft and deploy Microsoft Defender AV on all SharePoint servers.
    - If AMSI cannot be enabled, disconnect affected products from service that are public-facing on the internet until official mitigations are available. Once mitigations are provided, apply them according to CISA and vendor instructions.
    - Follow the applicable BOD 22-01 <https://www.cisa.gov/binding-operational-directive-22-01> guidance for cloud services or discontinue use of the product if mitigations are not available.
- For information on detection, prevention, and advanced threat hunting measures, see Microsoft's Disrupting active exploitation of on-premises SharePoint vulnerabilities <https://www.microsoft.com/en-us/security/blog/2025/07/22/disrupting-active-exploitation-of-on-premises-sharepoint-vulnerabilities/> and advisory <https://msrc.microsoft.com/update-guide/vulnerability/cve-2025-49706> for CVE-2025-49706. CISA encourages organizations to review all articles and security updates published by Microsoft on July 8, 2025, relevant to the SharePoint platform deployed in their environment.
- Rotate ASP.NET machine keys, then after applying Microsoft's security update, rotate ASP.NET machine keys again, and restart the IIS web server.
- Disconnect public-facing versions of SharePoint Server that have reached their end-of-life (EOL) or end-of-service (EOS) from the internet. For example, SharePoint Server 2013 and earlier versions are end-of-life and should be discontinued if still in use.
- Monitor for POSTs to `/_layouts/15/ToolPane.aspx?DisplayMode=Edit`
- Conduct scanning for IPs 107.191.58[.]76, 104.238.159[.]149, and 96.9.125[.]147, particularly between July 18-19, 2025.

- Update intrusion prevention system and web-application firewall (WAF) rules to block exploit patterns and anomalous behavior. For more information, see CISA's Guidance on SIEM and SOAR Implementation <https://www.cisa.gov/news-events/alerts/2025/05/27/new-guidance-siem-and-soar-implementation>.
- Implement comprehensive logging to identify exploitation activity. For more information, see CISA's Best Practices for Event Logging and Threat Detection <https://www.cisa.gov/resources-tools/resources/best-practices-event-logging-and-threat-detection>.
- Audit and minimize layout and admin privileges.

For more information on this vulnerability, please see Eye Security's reporting <https://research.eye.security/sharepoint-under-siege/> and Palo Alto Networks Unit42's post <https://unit42.paloaltonetworks.com/microsoft-sharepoint-cve-2025-49704-cve-2025-49706-cve-2025-53770/>. CVE-2025-53770 <https://nvd.nist.gov/vuln/detail/cve-2025-53770> was added to CISA's Known Exploited Vulnerabilities (KEV) catalog on July 20, 2025. **Update:** CVE-2025-49706 <https://nvd.nist.gov/vuln/detail/cve-2025-49706> and CVE-2025-49704 <https://nvd.nist.gov/vuln/detail/cve-2025-49704> were added to the KEV on July 22, 2025.

Note: This Alert may be updated to reflect new guidance issued by CISA or other parties.

CISA would like to acknowledge the contributions of the security researcher community in rapidly sharing insights that enabled CISA to notify critical infrastructure organizations impacted by this activity.

Organizations should report incidents and anomalous activity to CISA's 24/7 Operations Center at contact@mail.cisa.dhs.gov or (888) 282-0870.

Disclaimer:

The information in this report is being provided “as is” for informational purposes only. CISA does not endorse any commercial entity, product, company, or service, including any entities, products, or services linked within this document. Any reference to specific commercial entities, products, processes, or services by service mark, trademark, manufacturer, or otherwise, does not constitute or imply endorsement, recommendation, or favoring by CISA.

This product is provided subject to this Notification </notification> and this Privacy & Use </privacy-policy> policy.

Please share your thoughts

We recently updated our anonymous product survey; we welcome your feedback.

Return to top

Topics </topics> **Spotlight** </spotlight>

Resources & Tools </resources-tools> **News & Events** </news-events>

Careers </careers> **About** </about>

CISA Central

1-844-Say-CISA contact@mail.cisa.dhs.gov

CISA.gov
An official website of the U.S. Department of Homeland Security

About CISA </about>

Budget and Performance <https://www.dhs.gov/performance-financial-reports>

DHS.gov <https://www.dhs.gov>

FOIA Requ <https://w

No FEAR Act </no-fear-act>

Office of Inspector General <https://www.oig.dhs.gov/>

Privacy Policy </privacy-policy>

Subscribe

The White House <https://www.whitehouse.gov/>

USA.gov <https://www.usa.gov/>

Website Feedback </forms/feedback>