American Hospital Association™
Advancing Health in America

Cybersecurity Advisory

July 21, 2025

# Ongoing Attack Impacting Microsoft SharePoint Servers Managed on Premises

*Microsoft issues patches to help address issue; see CISA bulletin with additional details*

There is an ongoing attack targeting flaws in Microsoft's SharePoint server software. Microsoft has published guidance on protecting vulnerable systems, and these vulnerabilities only impact on-premises installations of SharePoint. Users whose data is in the Microsoft 365 Cloud are not impacted.

**Please share this Cybersecurity Advisory with your IT and cybersecurity teams. Hospitals should ensure that, if they have potentially vulnerable systems, they are updated as quickly as possible.**

## BACKGROUND

Microsoft was aware of two critical vulnerabilities (CVEs) in their SharePoint server software. These flaws, CVE-2025-53770 and CVE-2025-53771, were patched on July 15. After patching, attackers used two previously unknown (zero-day) flaws, known as ToolShell, to bypass the patches. Microsoft issued additional patches to address these issues in Microsoft SharePoint Server Subscription Edition and Microsoft SharePoint Server 2019. They are still working on a fix for Microsoft SharePoint Server 2016. **Microsoft also advised that if users could not enable recommended malware protection, they should disconnect their servers from the internet until a security update is available.**

Microsoft recommends the following actions:

1. Use supported versions of on-premises SharePoint Server.
2. Apply the latest security updates, including the July 2025 Security Update.
3. Ensure the Antimalware Scan Interface is turned on and configured correctly, with an appropriate antivirus solution such as Defender Antivirus.
4. Deploy Microsoft Defender for Endpoint protection or equivalent threat solutions.
5. Rotate SharePoint Server ASP.NET machine keys.

The Cybersecurity and Infrastructure Security Agency also has published a bulletin with additional technical details and indicators for technical threat hunters. It is important to note that these vulnerabilities only impact SharePoint instances managed on premises. If your SharePoint instance is in the cloud, you are not impacted by this issue. At this time, we are not aware of any specific hospitals impacted by this vulnerability, but hospitals are encouraged to ensure that any potentially vulnerable systems are

updated and malware protections are enabled. Hospitals using potentially vulnerable versions should be aware that Microsoft will end support for Microsoft SharePoint 2016 and 2019 on July 14, 2026, so organizations should begin planning to migrate off these systems.

## FURTHER QUESTIONS

For more information, please contact John Riggi, AHA national advisor for cybersecurity and risk, at jriggi@aha.org, or Scott Gee, AHA deputy national advisor for cybersecurity and risk, at sgee@aha.org.