**Client Alert: Active and Critical Security Concern for SharePoint**

[Amy S. Mushahwar](https://www.lowenstein.com/people/attorneys/amy-mushahwar), [Kathleen A. McGee](https://www.lowenstein.com/people/attorneys/kathleen-mcgee), [Ken Fishkin](https://www.lowenstein.com/people/management-team/ken-fishkin), [Cairon S. Overton](https://www.lowenstein.com/people/attorneys/cairon-overton)

On July 20, 2025, Microsoft and the Cybersecurity and Infrastructure Security Agency (CISA) issued urgent warnings about new, actively exploited vulnerabilities in Microsoft SharePoint Server. These vulnerabilities, known as ToolShell (CVE-2025-53770 and CVE-2025-53771), allow attackers to gain unauthorized access to SharePoint servers, potentially leading to data theft, malware installation, and further compromise of internal networks. The vulnerabilities affect supported versions of SharePoint Server, including 2016, 2019, and Subscription Edition, and are being used in real-world attacks. This issue does not impact cloud-based SharePoint accounts in Microsoft 365.

Organizations using SharePoint Server should act immediately. Microsoft has released emergency security updates to address these issues, and it is critical to apply these patches as soon as possible. If patching cannot be done right away, we recommend disconnecting affected servers from the internet to limit exposure. Additional steps, such as updating antivirus protections and rotating security keys, are also advised to help prevent further compromise.

Entities running unsupported versions of SharePoint, such as SharePoint 2013, face even greater risk and should disconnect these systems from the internet immediately. We strongly encourage all organizations to review their SharePoint environments, apply the latest security updates, and consult with IT and security professionals to ensure their systems are protected. For further guidance or assistance, please contact our team.