OpenVoiceNews U.S.

Transparent. Unbiased. Yours.

Microsoft Sounds Alarm on SharePoint Server Zero-Day Attack

July 21, 2025

— Categories: Defence & Security

Microsoft has issued an urgent alert warning businesses and government agencies of an ongoing “zero-day” cyberattack targeting on-premises SharePoint servers, which are widely used for internal document management and collaboration. The cloud-based SharePoint Online platform remains unaffected. This vulnerability allows malicious actors to

spoof legitimate users, granting unauthorized access to internal systems and sensitive data.

The identified flaw, officially tracked as CVE-2025-53770, has already been exploited in attacks on at least 75 servers, including systems in U.S. government networks and private sector organizations. The Department of Homeland Security's Cybersecurity and Infrastructure Security Agency (CISA) and the Federal Bureau of Investigation (FBI) are actively working with Microsoft to investigate and contain the threat, alongside cybersecurity partners across multiple countries.

The vulnerability was discovered on July 18 by security researchers from Eye Security during the Pwn2Own hacking competition. It allows attackers to steal credentials and cryptographic keys, potentially enabling long-term access even after systems are patched. This elevates the risk of sustained surveillance and data theft, particularly for organizations holding sensitive or classified information.

Microsoft has already released emergency patches for SharePoint Server 2019 and the SharePoint Subscription Edition, while a fix for SharePoint 2016 is currently under development. The company strongly advises administrators to immediately disconnect vulnerable servers from internet-facing networks or apply enhanced endpoint protection until full mitigation is confirmed.

Marci McCarthy, chair of CISA's Cybersecurity Advisory Committee, stated that compromised servers should be taken offline immediately and isolated from wider networks to prevent lateral movement by attackers. The guidance underscores the severity of the threat, especially for organizations that may not yet realize their systems have been breached.

Cybersecurity analysts warn that even patched systems may still be vulnerable if attackers have already extracted sensitive cryptographic materials. Adam Meyers, Senior Vice President at CrowdStrike, emphasized the ongoing risk: “Anyone operating an on-premises SharePoint instance needs to assume the possibility of credential compromise.”

The breach has affected not only U.S. government agencies but also international energy companies, academic institutions, and other high-value targets. The global scope of the attack illustrates the growing complexity of defending enterprise software in a rapidly evolving threat landscape.

As investigations continue, Microsoft and federal agencies are urging all affected organizations to prioritize updates, strengthen defenses, and conduct thorough forensic reviews. The incident serves as a sharp reminder that even trusted enterprise platforms can pose significant risks without vigilant, continuous cybersecurity efforts.