Global Cyberattack Hits Microsoft SharePoint Servers: Scope, Risks, and Response

Infosources™

July 21, 2025

A newly uncovered cyberattack has placed Microsoft under intense global scrutiny, once again exposing critical weaknesses in its software ecosystem. In a breach affecting U.S. federal and state agencies, as well as private sector organizations, hackers exploited a previously unknown vulnerability in Microsoft SharePoint Server to gain unauthorized access and execute remote commands. Traced to a Chinese state-affiliated threat group, the attack highlights not only the growing sophistication of cyber-espionage campaigns but also the systemic risks of overreliance on a single technology vendor. As the incident unfolds, questions are mounting about Microsoft's limited and delayed response, sparking broader concerns about security transparency, vendor accountability, and the resilience of digital infrastructure.

In recent days, a severe global cyberattack has exploited a zero-day vulnerability (CVE-2025-53770) in Microsoft SharePoint Server, compromising a wide array of targets including U.S. federal and state agencies, universities, energy firms, telecommunications providers, and European governments. The attack, attributed to a China-linked group, has so far breached at least 85 servers across 29 organizations worldwide. Affected entities include government bodies in the U.S., Spain, and Brazil, along with a local authority in Albuquerque.

Exploited Vulnerability and Attack Mechanics

The attackers leveraged an unauthenticated remote code execution flaw in on-premises SharePoint servers—excluding Microsoft's cloud platforms like Microsoft 365. They used cryptographic keys such as MachineKey, ValidationKey, and DecryptionKey to forge trusted __VIEWSTATE payloads, enabling persistent, stealthy access. These credentials allow hackers to impersonate legitimate users, escalate privileges, and regain entry even after patches are applied.

A secondary vulnerability, CVE-2025-49706, is being chained with the zero-day flaw to further elevate access via spoofed HTTP referer headers. This exploit chain, dubbed "ToolShell," has been confirmed in active use by security researchers at Eye Security and Palo Alto Networks' Unit 42.

Microsoft's Response: Criticism Over Scope and Speed

Microsoft has released a patch for only one version of SharePoint, leaving at least two widely used versions exposed. The company's interim advice—enabling AMSI, deploying Defender AV, or disconnecting vulnerable servers—fails to address the stolen cryptographic keys. Without key rotation, compromised systems remain exposed even after patching.

This limited and delayed response has drawn sharp criticism. Security experts and officials have noted Microsoft's recurring pattern of narrow fixes and lack of transparency, especially in light of previous high-profile breaches, such as the 2023 Chinese email espionage campaign.

U.S. Government and Industry Response

The Department of Homeland Security, through the Cybersecurity and Infrastructure Security Agency (CISA), has launched an emergency response, alerting Microsoft and affected organizations. CISA has added the vulnerability to its Known Exploited Vulnerabilities catalog and urged swift mitigation steps. Meanwhile, the Center for Internet Security notified around 100 institutions, including public schools and universities, during a six-hour emergency alert window.

The FBI is also investigating and working closely with federal partners. However, response efforts have been hampered by budget cuts and staffing reductions at CISA, reducing threat intelligence and incident response capabilities by 65%.

Operational Impact and Risks

The attack's operational impact is significant. Affected systems include document repositories, email servers, and internal communication platforms like Teams. In one case, a U.S. state legislature lost access to a public-facing document portal. The extent of data exfiltration remains unclear, though the theft of credentials and use of backdoors suggests a long-term espionage campaign rather than immediate data destruction.

Experts have warned that even patched systems remain vulnerable if cryptographic secrets are not rotated. Attackers are blending into normal SharePoint operations, using PowerShell scripts to plant ASPX shells and evade detection.

Broader Implications

This incident underscores systemic issues in supply chain security, the risks of software monocultures, and overreliance on single vendors like Microsoft for critical infrastructure. In response to wider concerns, Microsoft announced it would no longer use China-based engineers on Pentagon cloud contracts following investigative reports. As cyber professionals race to contain the damage, this breach highlights the urgent need for holistic security strategies—beyond patching—to address credential theft, lateral movement, and persistent threats across hybrid environments.