US Federal Judiciary System Breach

Article Summary:

At the beginning of August, POLITICO reported that the U.S. federal judiciary's Case Management/Electronic Case Files (CM/ECF) system had been hacked since at least July 2025. The breach resulted in the theft of source code from at least three federal district courts, along with sealed case data (Sakellariadis & Miller, 2025). The system was first rolled out in the mid-1990s as the courts' main case and file management system and includes a public-facing component, PACER, which provides limited access to unsealed information.

While the hackers remain unidentified, the vulnerabilities they exploited included weak authentication methods, inadequate security measures when querying sensitive data within the system, and a decentralized structure with inconsistent security measures. The courts' CM/ECF system operates locally in over 200 locations and is managed autonomously by each jurisdiction. Over the past five years, the system's security risks and weaknesses have repeatedly been brought to the attention of individual courts, but only limited action has been taken to address them. For example, in May 2025, the administrative authority overseeing the system announced the enforcement of two-factor authentication, though this has not yet been fully implemented across all instances.

According to Sakellariadis and Miller (2025), each of the more than 200 CM/ECF instances requires tailored security measures, continuous monitoring tools, and regular application of security patches. However, instead of implementing these improvements, many local management authorities chose to revert to pen-and-paper methods for handling sensitive materials.

This breach is suspected to be a follow-up of the 2020 judiciary cybersecurity breach due to the same vulnerabilities, but despite the lessons learned from 2020, systemic security measures were still not implemented by 2025 (Miller, 2022). Even the administrative authority overseeing the CM/ECF system did not enforce security measures until 2025.

Analysis:

Attack Vector:

The initial attack vector can be traced back to the SolarWinds Orion breach in 2020, during which the judiciary, as one of SolarWinds' clients, installed the compromised update (CyberTalents, 2025; Pham-Khan et al., 2021). The backdoor, known as "Sunburst," was embedded within the update targeting certain institutions like governments, this created the opening for hackers to get into the judiciary's system (Yavo, 2020). The backdoor checked the environment it was in to make sure it was a verified target organization with no security software or analysis tools before activating (Yavo, 2020). Sunburst enabled the attackers to gain remote access and deploy additional malware with elevated privileges into the judiciary's systems (Fortinet, 2025). Once inside, the hackers moved stealthily through the system, gathering information while remaining undetected.

Vulnerabilities Exploited:

The CM/ECF systems were outdated and contained well-known security gaps that hackers repeatedly exploited during the 2020 and 2025 attacks. These gaps included the lack of two-factor authentication and lack of security monitoring, which allowed attackers to move laterally through the system without detection. As a result, their presence remained unnoticed for an extended period of time.

Additionally, the systems were decentralized and managed individually, meaning that some instances had weaker security measures, and most lacked proper monitoring for security threats. This decentralization further contributed to the delayed detection and containment of the attacks. The SolarWinds compromised Orion update highlighted the third-party risk management gap in the judiciary's security system. The federal judiciary did not verify the SolarWinds update before installing it, thus paving the way for supply chain attacks.

Impact:

The impact of the cybersecurity attack was the theft of sealed case files and the CM/ECF system source code. The theft of sealed case files created personal risks for witnesses and corporate risks for companies involved in civil or criminal cases before these courts. Witnesses faced the danger of being targeted for their testimony against criminals, particularly in high-profile cases. Companies, on the other hand, risked the exposure of trade secrets, financial records, and other confidential information that may have been submitted to the courts as part of ongoing litigation.

With the theft of the CM/ECF system source code, hackers now have a comprehensive understanding of the system and its vulnerabilities. This enables hackers to traverse the system faster and more easily in future attacks. The hackers in both 2020 and 2025 attacks are suspected to be from Russia and the information that was stolen can provide insight into Russian cybercriminals being prosecuted in the U.S. (Sakellariadis & Miller, 2025).

Mitigation Strategies:

This attack could have been mitigated—or its impact reduced—through proactive security monitoring and centralized security management. Following the 2020 attack investigation, a proactive security team would have addressed the reported vulnerabilities, thereby preventing or lessening the impact of the 2025 attack and containing the damage more quickly. Furthermore, effective security monitoring would have enabled earlier detection and helped deter subsequent attacks.

Centralized cybersecurity management would have included the earlier and stricter enforcement of security measures and policies, incident management, disaster recovery and business continuity plans, and ensuring security patch updates across all system instances. The original backdoor installation attack could have been mitigated by stricter third-party risk management policies and procedures, including verifying updates before installing them.

Microsoft SharePoint “ToolShell” Ransomware Attack

Article Summary:

Microsoft’s SharePoint on-premise operations, which service over 400 organizations worldwide, were impacted by the “ToolShell” ransomware attack in July 2025 (Bouman, 2025). The attack exploited a combination of two vulnerabilities, CVE-2025-49704 and CVE-2025-49706, which allowed unauthorized access to SharePoint systems. Microsoft disclosed these vulnerabilities through its Microsoft Active Protections Program (MAPP). The MAPP program is designed to inform partners of vulnerabilities early so that they can implement security measures while a permanent fix is being developed (Hunt, 2025). According to Unit 42 at Palo Alto Networks (2025), proof-of-concept code for this exploitation had been posted to GitHub around the time the attack escalated into a significant active threat. Among the affected organizations were energy companies, healthcare providers, educational institutions, the U.S. Department of Education and the U.S. National Nuclear Security Administration (NNSA).

Attackers directly leveraged this combination of vulnerabilities to gain unauthorized access to SharePoint on-premise instances and deploy ransomware (Unit 42, 2025). Microsoft identified three threat actor groups from China that exploited these vulnerabilities prior to release of security patches(Hunt, 2025). Two of these groups are known for stealing intellectual property and conducting cyberespionage activities, while the third was responsible for deploying ransomware (Schwartz, 2025). Furthermore, although Microsoft acted quickly to identify and release security patches, Dutch cybersecurity firm Eye Security reported that “infections rose, suggesting that organizations hadn't installed the patch or . . . hadn't followed through [on the] mitigation advice detailed by Microsoft” (Schwartz, 2025). In response to the attack, Microsoft has tightened access within the MAPP program and restricted the scope of information it provides to partners (Hunt, 2025).

Analysis:

Attack Vector:

Through Microsoft’s Microsoft Active Protections Program (MAPP) information sharing of vulnerabilities and proof-of-concept code, the attackers were effectively provided with a roadmap and the necessary code to exploit vulnerabilities across all on-premise Microsoft SharePoint sites. Three threat actor groups capitalized on this opportunity. The hackers are potentially stealing information, which could enable more targeted phishing campaigns and impersonations of people or organizations (Bouman, 2025). The attackers exploited zero-day vulnerabilities in the Microsoft SharePoint sites.

Vulnerabilities Exploited:

The combination of two vulnerabilities, CVE-2025-49704 and CVE-2025-49706, along with the proof-of-concept code that Microsoft made available through its Microsoft Active Protections Program (MAPP), significantly escalated the rate of attack (Unit 42, 2025), possibly implicating members within the MAPP program.

Attackers still continue to exploit these vulnerabilities until security patches will be installed across all affected organizations. According to Schwartz (2025), Dutch cybersecurity firm Eye Security reported that “infections rose, suggesting that organizations hadn't installed the patch or . . . hadn't followed through [on the] mitigation advice detailed by Microsoft”. Microsoft’s clients were affected by this supply chain attack and vulnerabilities in their third-party risk management policies and procedures.

Impact:

Over 400 organizations worldwide were affected by the ransomware (Bouman, 2025), but the number of organizations that have paid ransom remains unknown. The impact continues to grow as many organizations have yet to apply the security patches and mitigation measures recommended by Microsoft. The full impact of this supply chain attack is not yet known because the vulnerabilities are still being exploited.

Mitigation Strategies:

The attack could have been mitigated by limiting the information shared with MAPP members and by further validating members’ intentions, especially given the prior leaks in 2012 and 2021 that stemmed from this program (Hunt, 2025). In the 2012 case, Microsoft identified an NDA breach within the MAPP program, while in 2021 the program was linked to the exploitation of specific known vulnerabilities.

Microsoft shares vulnerability details and proof-of-concept code with MAPP members in an effort to enable them to strengthen their systems while an official patch is developed. However, on multiple occasions this approach has backfired, suggesting that Microsoft should have revised its practices within the MAPP program. In addition, Microsoft’s clients should have a more robust third-party supply chain risk management program.

Comparative Analysis

Both of these incidents were examples of third-party risk and supply chain attacks. In the federal judiciary incident, SolarWinds Orion was their IT monitoring tool and the malware was inserted in their update. In the Microsoft SharePoint attack, Microsoft's clients were impacted as downstream users of SharePoint. In both cases, any clients who had active security monitoring and security programs in place were the least impacted. SolarWinds and Microsoft clients who actively pushed the security patches were secured from the attackers sooner than those who failed to heed the recommended mitigation procedures and install security patches. Both SolarWinds and Microsoft were proactive in remediating the problems and releasing security patches to their clients. Additionally, the attackers in both cases were foreign adversaries with the goal of disrupting service and cyberespionage. The judiciary incident stems from the SolarWinds attack which was broadly impacting many U.S. government organizations, critical infrastructure and industries, such as energy, telecommunications, healthcare, education and technology companies. Similarly, the Microsoft SharePoint attack affected similar organizations and companies. The Microsoft incident was partially also driven by money due to the use of ransomware whereas malware was used in the federal judiciary incident.

There are also differences between these two attacks. The SolarWinds attack involved the deliberate injection of malware to compromise downstream clients, while the Microsoft attack was characterized by the exploitation of zero-day vulnerabilities. The judiciary's systems lacked basic cybersecurity measures such as two-factor authentication, but SharePoint and its clients have cybersecurity programs in place with at least the basic security measures in place. Mitigation strategies between the two incidents are also different. In the federal judiciary case, active security program and monitoring procedures could have prevented the repeat attacks. In the SharePoint case, Microsoft's discretion regarding sharing sensitive vulnerability information outside the organization could have mitigated or prevented the attack. Both supply chain attacks were highly effective and both are still active threats. The full impact for both the judiciary and SharePoint cases is still developing since all impacted instances have yet to apply the security patches and the judiciary system's source code has been stolen.

Lessons Learned

Two primary points of concern that emerge from both instances are third-party risks and supply chain risks, which have not yet been managed effectively. These attacks underscore how vulnerable organizations remain to threats originating from their vendors, regardless of the strength of their own security perimeters. In the global industry, numerous vendors facilitate third-party interactions for organizations. Assessing these risks and evaluating the security posture of all vendors has become increasingly important as the capabilities vendors provide span multiple domains. Consequently, vendors become prime targets for foreign adversaries. Any deficiencies in the risk assessment and management of vendors can expose vulnerabilities across the entire supply chain and increase the likelihood of new attack vectors.

Moreover, both incidents demonstrate repetitive attacks that exploit the same vectors and vulnerabilities at their source, illustrating that sustained security vigilance is critical to deterring or preventing future compromises. When an incident occurs and subsequent investigations are completed, the resulting recommendations should be regarded with utmost seriousness, as unresolved vulnerabilities are highly likely to be exploited again. Microsoft experienced breaches in its MAPP program prior to 2025, and the federal judiciary encountered similar compromises in the past. Timely implementation of recommendations from earlier incidents could have deterred or even prevented the more recent attacks. Microsoft's prior breaches in the MAPP program should have prompted more ethical and secure handling of sensitive data, such as restricting the dissemination of vulnerability information until security patches were available. Fundamental security measures, which include two-factor authentication and active security monitoring, constitute powerful deterrents against attackers. These measures enabled the rapid detection and containment of the SharePoint attack, and they could likewise have mitigated or prevented the judiciary compromise. Implementing such measures for the federal judiciary, even in the aftermath of source code theft, can still enhance resilience against future attacks and enable earlier detection.

In conclusion, cybersecurity should not be perceived solely as the responsibility of the IT department, but rather as a collective obligation of all organizational units, integrated into every process and activity. Each unit handles distinct forms of sensitive data, and every employee within an organization needs to become a part of the security posture. Security is a shared responsibility, and only through collective vigilance can an organization's security posture and defensive perimeter be preserved effectively.

References:

Bouman, A. (2025, July 23). *The SharePoint flaw has now hit over 400 companies including a US nuclear administration*. Tom's Guide. https://www.tomsguide.com/computing/online-security/the-sharepoint-flaw-has-now-hit-over-400-companies-including-a-us-nuclear-administration

CyberTalents. (2025). *SolarWinds Attack: What you Need to Know*. CyberTalents Blog. https://cybertalents.com/blog/solarwinds-attack?utm_source=chatgpt.com

Fortinet. (2025). *SolarWinds Supply Chain Attack*. Fortinet. https://www.fortinet.com/resources/cyberglossary/solarwinds-cyber-attack

Hunt, C. (2025, August 21). *Microsoft just locked Chinese firms out of its cybersecurity program—Here's why*. Windows Central. https://www.windowscentral.com/microsoft/microsofts-cybersecurity-crackdown-is-here-a-response-to-beijing-linked-breaches

Miller, M. (2022, July 28). *Justice Department investigating data breach of federal court system*. POLITICO. https://www.politico.com/news/2022/07/28/justice-department-data-breach-federal-court-system-00048485

Pham-Khan, M., Szewczyk, G. P., & Yannella, P. N. (2021, January 13). Federal Court System—And Possibly Sealed Filings—Breached in Connection With SolarWinds Hack [CyberAdviser by the Privacy and Data Security Group at Ballard Spahr, LLP]. *CyberAdviser*. https://www.cyberadviserblog.com/2021/01/federal-court-system-and-possibly-sealed-filings-breached-in-connection-with-solarwinds-hack/

Sakellariadis, J., & Miller, M. (2025, August 12). *Hack of federal court filing system exploited security flaws known since 2020*. POLITICO. https://www.politico.com/news/2025/08/12/federal-courts-hack-security-flaw-00506392

Schwartz, M. J. (2025, July 29). *SharePoint Zero-Days Exploited to Unleash Warlock Ransomware*. https://www.bankinfosecurity.com/sharepoint-zero-days-exploited-to-unleash-warlock-ransomware-a-29073

Unit 42. (2025, July 31). Active Exploitation of Microsoft SharePoint Vulnerabilities: Threat Brief (Updated August 12). *Unit 42 by Palo Alto Networks*. https://unit42.paloaltonetworks.com/microsoft-sharepoint-cve-2025-49704-cve-2025-49706-cve-2025-53770/

Yavo, U. (2020, December 21). *What We Have Learned So Far about the “Sunburst”/SolarWinds Hack | FortiGuard labs*. Fortinet Blog. https://www.fortinet.com/blog/threat-research/what-we-have-learned-so-far-about-the-sunburst-solarwinds-hack