July 21, 2025

EMERGING THREATS

CVE-2025-53770 - Microsoft Sharepoint Mass Exploitation (ToolShell)

In July of 2025, large-scale exploitation of a vulnerability affecting Microsoft SharePoint servers was discovered by researchers. The campaign leverages a critical zero-day vulnerability in Microsoft SharePoint Server, tracked as CVE-2025-53770, to facilitate unauthorized remote code execution (RCE) on vulnerable on-premises servers. Furthermore, the vulnerability allows attackers to exploit deserialization of untrusted data, granting unauthenticated access to SharePoint systems. The exploitation chain, dubbed "ToolShell," has been actively utilized in large-scale attacks, compromising over 85 SharePoint servers across 29 organizations, including multinational corporations and government entities. The impact of this vulnerability is quite significant, because it enables attackers to execute arbitrary code, access sensitive data, and potentially move laterally within the network of targeted victims. Its exploitation underscores the critical need for timely patching and robust security measures to protect enterprise infrastructures in modern environments. Intel 471 will continue to update this collection with pertinent info as research continues and new data is uncovered.

THREAT SUMMARY

In July of 2025, large-scale exploitation of a vulnerability affecting Microsoft SharePoint servers was discovered by researchers. The campaign leverages a critical zero-day vulnerability in Microsoft SharePoint Server, tracked as CVE-2025-53770, to facilitate unauthorized remote code execution (RCE) on vulnerable on-premises servers.

Furthermore, the vulnerability allows attackers to exploit deserialization of untrusted data, granting unauthenticated access to SharePoint systems. The exploitation chain, dubbed "ToolShell," has been actively utilized in large-scale attacks, compromising over 85 SharePoint servers across 29 organizations, including multinational corporations and government entities. The impact of this vulnerability is quite significant, because it enables attackers to execute arbitrary code, access sensitive data, and potentially move laterally within the network of targeted victims. Its exploitation underscores the critical need for timely patching and robust security measures to protect enterprise infrastructures in modern environments. Intel 471 will continue to update this collection with pertinent info as research continues and new data is uncovered.

SYNOPSIS

CVE-2025-53770 is a critical vulnerability in Microsoft SharePoint Server, stemming from improper deserialization of untrusted data in the platform's processing logic. This flaw allows attackers to execute arbitrary code remotely on the server without requiring any authentication. The vulnerability is triggered when a specially crafted payload is sent to the SharePoint server, specifically targeting the ToolPane.aspx?DisplayMode=Edit endpoint. When SharePoint processes this input, the malicious data is deserialized and executed, granting the attacker unauthorized access to the system. The nature of this vulnerability allows the attacker to bypass SharePoint's authentication mechanisms, making it possible for an attacker to perform actions typically reserved for authenticated users, including deploying malicious payloads, exfiltrating sensitive data, or manipulating system configurations.

The exploitation of CVE-2025-53770 is particularly stealthy, as the malicious payload blends seamlessly with normal SharePoint traffic, evading detection by traditional network monitoring systems. Once the attacker gains access, they can use the compromised server to move laterally within the organization's network, gather intelligence, or deploy additional tools. Notably, the vulnerability has been linked to high-profile attacks, including the compromise of multiple SharePoint servers across industries. This makes the vulnerability highly impactful, especially for organizations relying heavily on SharePoint for internal communication and document management. As exploitation of this vulnerability continues in the wild, it is crucial for organizations to apply security patches, restrict external access to vulnerable endpoints, and implement advanced threat detection systems to monitor for suspicious activity related to this attack. Given the severity of this flaw, CVE-2025-53770 represents a significant risk to organizations that have not yet addressed the vulnerability.

HUNT PACKAGE COLLECTION

https://hunter.cyborgsecurity.io/research/search?state=(compatible:!f,filters:(),library:!(cyborg_collections),page:0,size:10,sort:last_updated_desc,term:!('939f2b46-0445-41c5-8d84-46ab4184cb12'),touched:!t)

RELATED HUNT PACKAGES

SUSPECT CHILD PROCESS TO IIS WORKER PROCESS (W3WP.EXE) - POTENTIAL EXPLOITATION

https://hunter.cyborgsecurity.io/details/use-case/667c9f6c-8e41-4309-80a8-55fc3c5769bf

Environmentally Unique ASPX File Written to \TEMPLATE\LAYOUTS\ - Potential Webshell Installation

https://hunter.cyborgsecurity.io/details/use-case/f11f03b1-f725-4c17-9bdd-04dd2b62b3e4

POWERSHELL ENCODED COMMAND EXECUTION

https://hunter.cyborgsecurity.io/details/use-case/d2d3bbc2-6e57-4043-ab24-988a6a6c88db

MITRE CONTEXT

- Exploits Vulnerabilities:
  - CVE-2025-53770
- MITRE Tactic Names:
  - Lateral Movement
  - Defense Evasion
  - Execution
  - Persistence
  - Initial Access
- MITRE Technique Names:
  - Web Shell
  - Exploit Public-Facing Application
  - Exploitation of Remote Services
  - Obfuscated Files or Information
  - PowerShell
- Threat Names:
  - ToolShell
  - SharpyShell

TITAN REFERENCE

1. TITAN Finished Intel Report - Microsoft SharePoint zero-day remote code execution vulnerabilities exploited: https://titan.intel471.com/report/fintel/2a91f6a2dde6f65cd3613886b122ba0a

ADDITIONAL REFERENCES

1. https://research.eye.security/sharepoint-under-siege/
2. https://msrc.microsoft.com/blog/2025/07/customer-guidance-for-sharepoint-vulnerability-cve-2025-53770/
3. https://www.cisa.gov/news-events/alerts/2025/07/20/cisa-adds-one-known-exploited-vulnerability-cve-2025-53770-toolshell-catalog
4. https://thehackernews.com/2025/07/critical-microsoft-sharepoint-flaw.html