



< click to listen to this article

NEWS

# SharePoint Zero Day Vulnerability Exploited in Government System Breaches

By Chris Paoli | 07/21/2025

The U.S. Cybersecurity and Infrastructure Security Agency (CISA) **issued an alert Sunday** detailing active exploitation of a critical SharePoint vulnerability, CVE-2025-53770.

The zero-day flaw has reportedly been used to breach multiple government systems and remains a significant threat to unpatched on-premises SharePoint deployments. According to the advisory, the flaw is tied to a deserialization issue that allows unauthenticated remote code execution. Attackers can exploit the flaw to extract MachineKey configuration values, including the validationKey and decryptionKey, which enable them to forge authentication tokens and execute arbitrary code remotely.

MOST POPULAR

More than 9,000 externally accessible SharePoint servers are at risk, according to security firm Tenable. Microsoft released patches for SharePoint Server 2019 and SharePoint Subscription Edition late on July 20. A patch for SharePoint Server 2016 is expected soon.

"We've been coordinating closely with CISA, DOD Cyber Defense Command and key cybersecurity partners globally throughout our response," said a Microsoft spokesman, adding that the company has released out-of-band security updates.

Satnam Narang, senior staff research engineer at Tenable, said the fallout of the ongoing attacks could be substantial.

"The active exploitation of the SharePoint zero-day vulnerability over the weekend will have far reaching consequences for those organizations that were affected," Narang said. "Attackers were able to exploit the flaw, now identified as CVE-2025-53770, to steal MachineKey configuration details from vulnerable SharePoint Servers, which includes both a validationKey and a decryptionKey."

**NEW:  
KnowBe4  
Defend  
Integrates  
With  
Microsoft  
Defender for  
Office 365**

**FIND OUT HOW**

KnowBe4 Microsoft

Narang added that attackers can then craft requests to achieve unauthenticated remote code execution. He recommended looking for a suspicious file named `spinstall.aspx` on SharePoint servers, though the file may appear with other extensions.

Tenable advised organizations to begin incident response efforts immediately and to apply available patches while monitoring Microsoft's guidance for additional mitigations.

Adam Maurer, COO of Connecting Software, emphasized the importance of both software patching and physical architecture improvements.

"This day-one exploit of Microsoft's systems resulted from a massive and overlooked vulnerability that allowed attackers to execute arbitrary code remotely on unpatched on-premises SharePoint servers across several key sectors," Maurer said.

"It exploited a deserialization flaw within Microsoft's code, enabling attackers to gain control and access sensitive data," he added.

Maurer recommended air-gapped networks and data diodes to physically restrict access between sensitive servers and external networks.

"If they had been used in this instance, it could have prevented key sensitive information from being exfiltrated through the network, given that the SharePoint server itself would have had no direct network connection to external untrusted networks such as the internet," he said.

He further stressed the importance of pairing physical architecture with zero-trust configurations to block inbound traffic from untrusted sources.

Recommended actions for IT teams include:

- Apply the latest Microsoft patches for SharePoint 2019 and Subscription Edition.
- Monitor for the release of SharePoint 2016 patches.
- Investigate systems for the presence of spinstallo.aspx or other anomalies.
- Rotate cryptographic keys and invalidate sessions on affected servers.
- Evaluate network segmentation and firewall rules around SharePoint deployments.

#### About the Author

**Chris Paoli** (@ChrisPaoli5) is the associate editor for Converge360.

## Featured

### SharePoint Zero Day Vulnerability Exploited in Government System Breaches

The U.S. Cybersecurity and Infrastructure Security Agency (CISA) issued an alert Sunday detailing active exploitation of a critical SharePoint vulnerability, CVE-2025-53770.



### Restoring a File from a Windows



## Image Backup

PowerShell recovery scripts using WBAdmin no longer work in Windows 11, but VHDX mounting offers a manual workaround for restoring files.



## New Email Security Transparency Dashboard for Office 365 Defender

Microsoft has introduced a new Email Security Transparency Dashboard in Microsoft Defender for Office 365, offering customers visibility into threat detection metrics and benchmarking data.



## Take Control of Your Cloud Bill: Cost Models, Discounts and Hidden Fees Explained

As cloud costs grow more complex, understanding fixed vs. variable pricing, spotting hidden charges and using the right discount strategies are essential to keeping budgets on track.



## Microsoft Brings Autonomous AI Research to Azure with Deep Research Agents

Microsoft is transforming its AI research capabilities into enterprise-grade infrastructure with the limited preview launch of enhanced agent support in Azure AI Foundry.



Please enable JavaScript to view the [comments powered by Disqus.](#) [comments powered by Disqus](#)

An error occurred.

Try watching this video on [www.youtube.com](http://www.youtube.com), or enable JavaScript if it is disabled in your browser.

## SUBSCRIBE ON YOUTUBE



## Office 365 Watch

Sign up for our newsletter.

Email Address\*

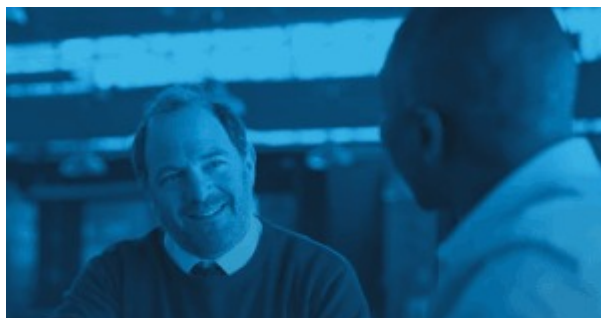
Country\*

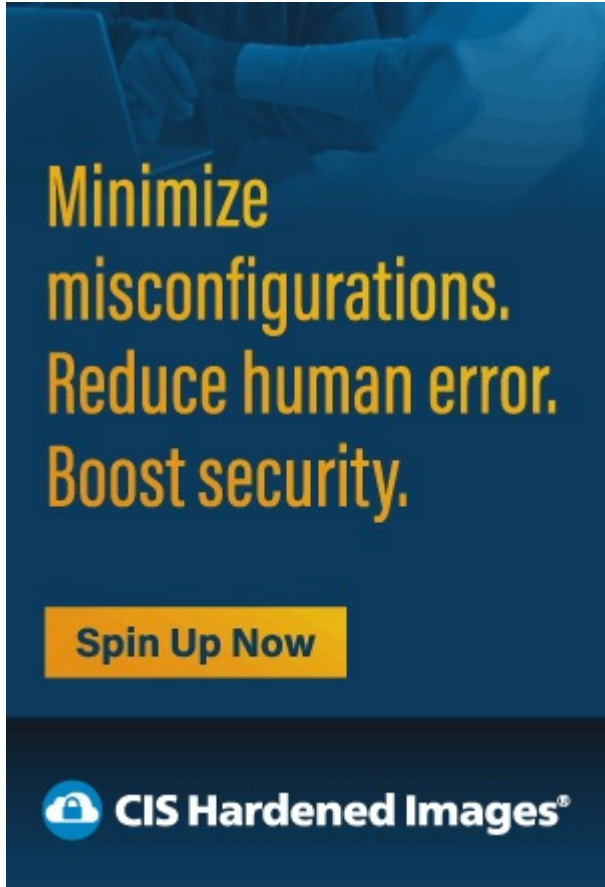
I agree to this site's [Privacy Policy](#)



Please type the letters/numbers you see above.


SUBMIT





**Minimize  
misconfigurations.  
Reduce human error.  
Boost security.**

**Spin Up Now**

 **CIS Hardened Images®**

## **MOST POPULAR ARTICLES**

**New Email Security Transparency Dashboard for Office 365 Defender**



**SharePoint Zero Day Vulnerability Exploited in Government System Breaches**



**Microsoft Throws Exchange Server 2016 and 2019 a Support Lifeline**



**Microsoft Intune and Entra Receives Security Copilot Enhancement**



**Restoring a File from a Windows Image Backup**





**Leverage VMs  
with extra  
security.**

[Learn More](#)

  **CIS Hardened  
Images®**

## UPCOMING TRAINING EVENTS

**Securing IT in the AI Era**  
July 23, 2025



**TechMentor @ Microsoft HQ**  
August 11-15, 2025



**Microsoft 365 Security Masterclass**  
August 25-26, 2025



**Live! 360 2-Day Hands-On Seminar: Swimming in the Lakes of Microsoft Fabric and AI**

**– A Hands-on Experience**  
September 18-19, 2025



**Live! 360 Orlando**  
November 16-21, 2025



**Artificial Intelligence Live! Orlando**  
November 16-21, 2025



**Cloud & Containers Live! Orlando**  
November 16-21, 2025



**Cybersecurity & Ransomware Live! Orlando**  
November 16-21, 2025



**Data Platform Live! Orlando**  
November 16-21, 2025



**TechMentor Orlando**  
November 16-21, 2025

## **WEBCASTS**

**The Overlooked Risk in Your Microsoft 365 Defense: Identity Protection**



**Manage & Secure Microsoft 365 Like an Expert Summit**



**Agentic AI Ransomware: What You Need to Know**

---



**Rally For Resilience**

---



**More Webcasts**

## **WHITEPAPERS**

**Beyond Passwords: A Guide to Advanced Enterprise Security Protection**

---



**G2 Grid Report for Security Awareness Training**

---



**Frost Radar for Human Risk Management**

---



**From Risk to Return - How KnowBe4 Helps Deliver Measurable ROI**

---



**More Tech Library**



and  
**compliance-  
focused.**

**LAUNCH NOW**

 **CIS Hardened Images®**



**Cost-effective  
and  
compliance-  
focused.**

**LAUNCH NOW**

 **CIS Hardened Images®**



**NEW!** Data Quality  
for Azure Data Factory

**Get Started**

**melissa**



An **IIO5**MEDIA<sup>2</sup> Company

**AI Boardroom**

**ADTmag**

**AWS Insider**

**Campus Security Today**

**Campus Technology**

**Environmental Protection**

**Live! 360**

**MCPmag**

**MedCloudInsider**

**Occupational Health & Safety**

**Pure AI**

**Redmond Channel Partner**

**Security Today**

**Spaces 4 Learning**

**TechMentor**

**Tech Tactics in Education**

**THE Journal**

**Virtualization & Cloud Review**

**Visual Studio Magazine**

**Visual Studio Live!**



© **1105 Media Inc.** See our **Privacy Policy**, **Cookie Policy** and **Terms of Use**. **CA: Do Not Sell My Personal Info**  
**Problems? Questions? Feedback? E-mail us.**