#### NATIONAL VULNERABILITY DATABASE



VULNERABILITIES

# **₩CVE-2025-49706 Detail**

#### **MODIFIED**

This CVE record has been updated after NVD enrichment efforts were completed. Enrichment data supplied by the NVD may require amendment due to these changes.

#### **Current Description**

Improper authentication in Microsoft Office SharePoint allows an unauthorized attacker to perform spoofing over a network

+View Analysis Description

Metrics CVSS Version 4.0 CVSS Version 3.x CVSS Version 2.0

NVD enrichment efforts reference publicly available information to associate vector strings. CVSS information contributed by other sources is also displayed.

**CVSS 3.x Severity and Vector Strings:** 

**CNA:** Microsoft Corporation

Base Score: 6.5 MEDIUM

Vector:

CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:N

## References to Advisories, Solutions, and Tools

By selecting these links, you will be leaving NIST webspace. We have provided these links to other web sites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other web sites that are more appropriate for your purpose. NIST does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, NIST does not endorse any commercial products that may be mentioned on these sites. Please address comments about this page to nvd@nist.gov.

Hyperlink	Resource
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-49706	Vendor Advisory
https://www.microsoft.com/en-us/security/blog/2025/07/22/disrupting-active-exploitation-of-on-premises-sharepoint-vulnerabilities/	

## This CVE is in CISA's Known Exploited Vulnerabilities Catalog

Reference CISA's BOD 22-01 and Known Exploited Vulnerabilities Catalog for further guidance and requirements.

<b>Vulnerability Name</b>	Date Added	Due Date	Required Action
Microsoft SharePoint Improper Authentication Vulnerability	07/22/2025		CISA recommends disconnecting public-facing versions of SharePoint Server that have reached their end-of-life (EOL) or end-of-service (EOS). For example, SharePoint Server 2013 and earlier versions are end-of-life and should be discontinued if still in use. For supported versions, please follow the mitigations according to CISA and vendor instructions. Adhere to the applicable BOD 22-01 guidance

#### **QUICK INFO**

**CVE Dictionary Entry:** 

CVE-2025-49706

**NVD Published Date:** 

07/08/2025

**NVD Last Modified:** 

07/22/2025

Source:

Microsoft Corporation

for cloud services or discontinue use of the product if mitigations are not available.

#### **Weakness Enumeration**

CWE-ID	CWE Name	Source
CWE-287	Improper Authentication	Microsoft Corporation

## **Known Affected Software Configurations** Switch to CPE 2.2

Configuration 1 (hide)

\* cpe:2.3:a:microsoft:sharepoint\_enterprise\_server:2016:\*:\*:\*:\*:\*:\*: Show Matching CPE(s)▼ Up to (excluding) cpe:2.3:a:microsoft:sharepoint\_server:\*:\*:\*:subscription:\*:\*:\* Show Matching CPE(s).▼ 16.0.18526.20424 # cpe:2.3:a:microsoft:sharepoint\_server:2019:\*:\*:\*:\*:\*:\*:\* Show Matching CPE(s)▼

₩ Denotes Vulnerable Software

Are we missing a CPE here? Please let us know.

### **Change History**

6 change records found show changes













**HEADQUARTERS** 

100 Bureau Drive Gaithersburg, MD 20899 (301) 975-2000

Webmaster | Contact Us | Our Other Offices

Incident Response Assistance and Non-NVD Re Technical Cyber Security Ques

US-CERT Security Operations ( Email: soc@us-ce Phone: 1-888-282

te Privacy | Accessibility | Privacy Program | Copyrights | Vulnerability Disclosure | No Fear Act Policy | FOIA | Environmental Policy | Scientific Integrity | Information Quality Standards | Comn Science.gov | USA.gov