



# Microsoft SharePoint Server Spoofing Vulnerability

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF](#) 

## Summary

<b>CVE</b>	CVE-2026-32201
<b>State</b>	PUBLISHED
<b>Assigner</b>	microsoft
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2026-04-14 18:17:27 UTC
<b>Updated</b>	2026-04-14 19:37:08 UTC
<b>Description</b>	Improper input validation in Microsoft Office SharePoint allows an unauthorized attacker to perform spoofing over a network

## Risk And Classification

**Primary CVSS:** v3.1 6.5 MEDIUM from secure@microsoft.com

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

**EPSS:** 0.008080000 probability, percentile 0.742410000 (date 2026-04-16)

**CISA KEV:** Listed on 2026-04-14; due 2026-04-28; ransomware use Unknown

**Problem Types:** CWE-20 | CWE-20 CWE-20: Improper Input Validation

Version	Source	Type	Score	Severity	Vector
3.1	secure@microsoft.com	Primary	6.5	MEDIUM	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:N
3.1	CNA	CVSS	6.5	MEDIUM	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:N/E:F/RL:O/RC:C

## CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

None

User Interaction

None

Scope

Unchanged

Confidentiality

Low

Integrity

Low

Availability

None

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

### CISA Known Exploited Vulnerability

<b>Vendor</b>	Microsoft
<b>Product</b>	SharePoint Server
<b>Name</b>	Microsoft SharePoint Server Improper Input Validation Vulnerability
<b>Required Action</b>	Apply mitigations per vendor instructions, follow applicable BOD 22-01 guidance for cloud services, or discontinue use of the product if mitigations are unavailable.
<b>Notes</b>	<a href="https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2026-32201">https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2026-32201</a> ; <a href="https://nvd.nist.gov/vuln/detail/CVE-2026-32201">https://nvd.nist.gov/vuln/detail/CVE-2026-32201</a>

### NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Microsoft	Sharepoint Server	All	All	All	All
Application	Microsoft	Sharepoint Server	2016	All	All	All
Application	Microsoft	Sharepoint Server	2019	All	All	All

### Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Microsoft	Microsoft SharePoint Enterprise Server 2016	affected 16.0.0 16.0.5548.1003 custom	x64-based Systems
CNA	Microsoft	Microsoft SharePoint Server 2019	affected 16.0.0 16.0.10417.20114 custom	x64-based Systems
CNA	Microsoft	Microsoft SharePoint Server Subscription Edition	affected 16.0.0 16.0.19725.20210 custom	x64-based Systems

### References

Reference	Source	Link	Tags
<a href="https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-32201">msrc.microsoft.com/update-guide/vulnerability/CVE-2026-32201</a>	secure@microsoft.com	<a href="https://msrc.microsoft.com">msrc.microsoft.com</a>	Vendor /
<a href="https://www.cisa.gov/known-exploited-vulnerabilities-catalog">www.cisa.gov/known-exploited-vulnerabilities-catalog</a>	134c704f-9b21-4f2e-91b3-4a467353bcc0	<a href="https://www.cisa.gov">www.cisa.gov</a>	US Govern
CVE Program record	CVE.ORG	<a href="https://www.cve.org">www.cve.org</a>	canonical
NVD vulnerability detail	NVD	<a href="https://nvd.nist.gov">nvd.nist.gov</a>	canonical
CISA Known Exploited Vulnerabilities catalog	CISA	<a href="https://www.cisa.gov">www.cisa.gov</a>	kev

No vendor comments have been submitted for this CVE.

There are currently no legacy CID mappings associated with this CVE.

There are currently no legacy QID mappings associated with this CVE.

© [CVE.report](#) 2026 |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

**Free CVE JSON API** [cve.report/api](#)

**CVE.report and Source URL Uptime Status** [status.cve.report](#)