Microsoft SharePoint Server Remote Code Execution Vulnerability

MITRE | NVD | CVE.ORG | JSON API | Print: PDF

Summary

CVE	CVE-2026-40365
State	PUBLISHED
Assigner	microsoft
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-05-12 18:17:15 UTC
Updated	2026-05-13 20:52:35 UTC
Description	Insufficient granularity of access control in Microsoft Office SharePoint allows an authorized attacker to execute code over a

Risk And Classification

Primary CVSS: v3.1 8.8 HIGH from secure@microsoft.com

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

EPSS: 0.000630000 probability, percentile 0.197060000 (date 2026-05-15)

Problem Types: CWE-1220 | CWE-1220 CWE-1220: Insufficient Granularity of Access Control

Version	Source	Type	Score	Severity	Vector
3.1	secure@microsoft.com	Primary	8.8	HIGH	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H
3.1	CNA	CVSS	8.8	HIGH	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C

CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

Low

User Interaction

None

Scope

Unchanged

Confidentiality

High

ntegrity

High

Availability

High

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

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 16.0.5552.1002 custom	x64-based Systems
CNA	Microsoft	Microsoft SharePoint Server 2019	affected 16.0.0 16.0.10417.20128 custom	x64-based Systems
CNA	Microsoft	Microsoft SharePoint Server Subscription Edition	affected 16.0.0 16.0.19725.20280 custom	x64-based Systems

References

Reference	Source	Link	Tags
msrc.microsoft.com/update-guide/vulnerability/CVE-2026-40365	secure@microsoft.com	msrc.microsoft.com	Vendor Advisory
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, analysis

No vendor comments have been submitted for 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 registred 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**