



CVE-2018-1005

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

Summary

CVE	CVE-2018-1005
State	PUBLIC
Assigner	secure@microsoft.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2018-04-12 01:29:00 UTC
Updated	2019-10-03 00:03:00 UTC
Description	An elevation of privilege vulnerability exists when Microsoft SharePoint Server does not properly sanitize a specially crafted

Risk And Classification

Problem Types: CWE-79

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Microsoft	Sharepoint Enterprise Server	2013	sp1	All	All
Application	Microsoft	Sharepoint Enterprise Server	2016	All	All	All
Application	Microsoft	Sharepoint Enterprise Server	2013	sp1	All	All
Application	Microsoft	Sharepoint Enterprise Server	2016	All	All	All

References

Reference
portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-1005
Microsoft SharePoint Server CVE-2018-1005 Remote Privilege Escalation Vulnerability
Microsoft SharePoint Server Input Validation Flaw Lets Remote Authenticated Users Conduct Cross-Site Scripting Attacks - SecurityTracker
CVE Program record
NVD vulnerability detail

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 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](#)