



# Microsoft Power Apps Spoofing Vulnerability

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF !\[\]\(003082e50e3009141f59bd5df831749f\_img.jpg\)](#)

## Summary

<b>CVE</b>	CVE-2026-26149
<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 18:16:45 UTC
<b>Updated</b>	2026-04-20 21:16:08 UTC
<b>Description</b>	Improper neutralization of escape, meta, or control sequences in Microsoft Power Apps allows an authorized attacker to per

## Risk And Classification

**Primary CVSS:** v3.1 9 CRITICAL from secure@microsoft.com

[CVSS:3.1/AV:N/AC:L/PR:L/UI:R/S:C/C:H/I:H/A:H](#)

**EPSS:** 0.000580000 probability, percentile 0.181460000 (date 2026-04-20)

**Problem Types:** CWE-150 | CWE-150 CWE-150: Improper Neutralization of Escape, Meta, or Control Sequences

Version	Source	Type	Score	Severity	Vector
3.1	secure@microsoft.com	Secondary	9	CRITICAL	<a href="#">CVSS:3.1/AV:N/AC:L/PR:L/UI:R/S:C/C:H/I:H/A:H</a>
3.1	CNA	CVSS	9	CRITICAL	<a href="#">CVSS:3.1/AV:N/AC:L/PR:L/UI:R/S:C/C:H/I:H/A:H/E:U/RL:T/RC:C</a>

## CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

Low

User Interaction

Required

Scope

Changed

Confidentiality

High

ntegrity

High

Availability

High

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

### Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Microsoft	Microsoft Power Apps	affected 1710 (9.2.23071.136) 3.26032.10.0 custom	Not specified

### References

Reference	Source	Link	Tags
msrc.microsoft.com/update-guide/vulnerability/CVE-2026-26149	secure@microsoft.com	msrc.microsoft.com	
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 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](https://cve.report/api)

CVE.report and Source URL Uptime Status [status.cve.report](https://status.cve.report)