Microsoft Power Apps Spoofing Vulnerability

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

Summary

CVE	CVE-2026-26149
State	PUBLISHED
Assigner	microsoft
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-04-14 18:16:45 UTC
Updated	2026-04-20 21:16:08 UTC
Description	Improper neutralization of escape, meta, or control sequences in Microsoft Power Apps allows an authorized attacker to pe

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	CVSS:3.1/AV:N/AC:L/PR:L/UI:R/S:C/C:H/I:H/A:H
3.1	CNA	CVSS	9	CRITICAL	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

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.