



WordPress Breakdance plugin <= 1.7.2 - Authenticated Remote Code Execution (RCE) vulnerability

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

Summary

CVE	CVE-2024-31390
State	PUBLISHED
Assigner	Patchstack
Source Priority	CVE Program / NVD first with legacy fallback
Published	2024-04-03 12:15:14 UTC
Updated	2026-04-28 19:24:28 UTC

Description : Improper Control of Generation of Code ('Code Injection') vulnerability in Soflyy Breakdance allows : Code Injection.This is

Risk And Classification

Primary CVSS: v3.1 9.9 CRITICAL from audit@patchstack.com

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

EPSS: 0.001410000 probability, percentile 0.338200000 (date 2026-04-28)

Problem Types: CWE-94 | CWE-94 CWE-94: Improper Control of Generation of Code ('Code Injection')

Version	Source	Type	Score	Severity	Vector
3.1	audit@patchstack.com	Secondary	9.9	CRITICAL	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:H
3.1	CNA	CVSS	9.9	CRITICAL	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:H

CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

Low

User Interaction

None

Scope

Changed

Confidentiality

High

Integrity

High

Availability

High

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

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Soflyy	Breakdance	affected n/a 1.7.2 custom	Not specified

References

Reference	Source
WordPress Breakdance plugin <= 1.7.0 - Authenticated Remote Code Execution (RCE) vulnerability - Patchstack	af854a3a-2127-422b-91a
Client Mode Remote Code Execution – Breakdance <= 1.7.0 – CVE-2024-31390 – snicco	af854a3a-2127-422b-91a
patchstack.com/articles/unpatched-authenticated-rce-in-oxygen-and-breakdance...	af854a3a-2127-422b-91a
www.youtube.com/watch	af854a3a-2127-422b-91a
CVE Program record	CVE.ORG
NVD vulnerability detail	NVD

Vendor Comments And Credit

Discovery Credit

CNA: [Snicco \(Patchstack Alliance\)](#) (en)

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](#)