



soundcloud-rpc: Remote Code Execution via XSS in Track Title

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

Summary

CVE	CVE-2026-44482
State	PUBLISHED
Assigner	GitHub_M
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-05-14 15:16:48 UTC
Updated	2026-05-14 18:19:25 UTC
Description	soundcloud-rpc is a SoundCloud Client with Discord Rich Presence, Dark Mode, Last.fm and Adblock support. Prior to 0.1.

Risk And Classification

Primary CVSS: v3.1 9.6 CRITICAL from security-advisories@github.com

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

Problem Types: CWE-20 | CWE-79 | CWE-94 | CWE-862 | CWE-20 CWE-20: Improper Input Validation | CWE-79 CWE-79: Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') | CWE-94 CWE-94: Improper Control of Generation of Code ('Code Injection') | CWE-862 CWE-862: Missing Authorization

Version	Source	Type	Score	Severity	Vector
3.1	security-advisories@github.com	Secondary	9.6	CRITICAL	CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:H/I:H/A:H
3.1	CNA	DECLARED	9.6	CRITICAL	CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:H/I:H/A:H

CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

None

User Interaction

Required

Scope

Changed

Confidentiality

Confidentiality

High

Integrity

High

Availability

High

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

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Richardhbtz	Soundcloud-rpc	affected < 0.1.8	Not specified

References

Reference	Source	Link
github.com/richardhbtz/soundcloud-rpc/security/advisories/GHSA-p37x-32p8...	134c704f-9b21-4f2e-91b3-4a467353bcc0	github.com
CVE Program record	CVE.ORG	www.cve.org
NVD vulnerability detail	NVD	nvd.nist.gov

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