

Security Reconnaissance Report

Target: soundcloud.com

Scan ID: c6da41d9-f730-4d3c-8eb4-48755a373124

Date: 2025-04-23 02:19:11

Status: complete

Executive Summary

Risk Score	Critical	High	Medium	Low	Total
High	0	1	2	2	5

Domain Dns

Domain Information

Domain	soundcloud.com
IP Address	18.154.185.72
Location	
Hosting	

WHOIS Information

Registrar	GANDI SAS
Created	2005-07-25T10:33:38
Updated	2024-09-03T16:39:07
Expires	2025-06-08T03:59:59

DNS Records

A Records

18.154.185.9
18.154.185.72
18.154.185.22
18.154.185.39

MX Records

50 aspmx3.googlemail.com.
10 aspmx.l.google.com.
20 alt1.aspmx.l.google.com.

20 alt2.aspx.l.google.com.
50 aspmx2.googlemail.com.

NS Records

ns-1445.awsdns-52.org.
ns-1745.awsdns-26.co.uk.
ns-56.awsdns-07.com.
ns-799.awsdns-35.net.

TXT Records

"MS=ms67894313"
"ZOOM_verify_hBlTOUUcSiW7IhDAv16bqQ"
"apple-domain-verification=DJEx73gNNUTjejVL"
"asv=f854ad6e866ab7a88b57bebd971f158b"
"atlassian-domain-verification=fycZUT0eVlPEiaehQXOKmXCe9NJJeJsZmCWgWfW7GSuras9JTdhCVrebn8zfRIQ3v"
"botify-site-verification=VyJVacuqlVARp4iXaeza0p9iFlTUubb"
"d24wuv6owifbwc.cloudfront.net"
"datadome-domain-verify=gf9iUK5M4yfQc3zyEW1aXklGOXdhjLyy"
"google-site-verification=SdIX4P8Pq06U6a0DMUEvgI5rQS7RM0Z33zKcet-iVf8"
"google-site-verification=U41CuhcP0HS0kVo6HaaLA0Vo-6Wdk8YO-M_Q4rukDmU"
"google-site-verification=bGedCZYrMEPIXRPH5n3Rb0dJjFPACxUP_xMbAPCPenU"
"google-site-verification=ise_yQfK5npT23y4X7QB1-WYgNjA7AuUrRQqo1Q66EU"
"miro-verification=f08757fb9739f5263de5643f8c9534cccb49b7d3"
"onetrust-domain-verification=f110ce3d05314cfb8054ab5e0903ff68"
"postman-domain-verification=5b7709a2c59b36a8a43b9ac9dfce70486e48a77ead9bc6796eb6d23405f1e97d248fcea57dca123555ac56280fda66895e29ba3a9a0f2c6c400985776f040d5a"
"proxy-ssl.webflow.com"
"stripe-verification=e1469db8bb5c9886c8a7abbece38ddc342618aa4ac7dca85b73731668ea5ec70"
"v=spf1 include:_spf.google.com ip4:178.249.138.0/23 ip4:145.253.129.216/29 ip4:80.82.202.192/28 ip4:52.17.172.90/32 include:spf.mandrillapp.com include:7303199.spf04.hubspotemail.net include:spf.extole.io -all"
"wrQAupWCtBhVn8GcFVpM6CMH--bBTLOI "
"JlHKdOBLZpjs/UOfcGHRiSM38ADQhJ0fAN6IMMgSdts="
"MS=ms25371803"

SOA Records

ns-799.awsdns-35.net. awsdns-hostmaster.amazon.com. 1 7200 900 1209600 86400

SSL/TLS Information

Issuer	GlobalSign nv-sa
Subject	*.soundcloud.com
Valid Until	Mar 16 10:31:57 2026 GMT
Grade	A

Tech Stack

Server Information

Web Server	am/2
CMS	
Database	
Operating System	

Ports Network

Open Ports

Port	Service
80	http
443	https

Files Directories

Sensitive Files

File	Sensitivity Level
robots.txt	low
sitemap.xml	low
server-status	low
server-info	low
crossdomain.xml	low

Discovered Directories

- admin
- administrator
- backup
- backups
- config
- db
- default
- files
- home
- img
- install
- log
- login

- logs
- old
- panel
- root
- setup
- site
- staging
- temp
- tmp
- upload
- uploads
- user
- web
- wp-admin

Api Endpoints

API Configuration

Authentication	Unknown
CORS	Unknown
Swagger/OpenAPI	Available
GraphQL	Not found

Js Analysis

Potential Secrets

Type	File	Value
Secret	0-64499ab3.js	onTo...lick
API Key	49-f5449dda.js	1403...459e
API Key	49-f5449dda.js	a730...6d2a
AWS Key	49-f5449dda.js	agPa...ment

Dependencies

Package	Usage Count
util	2

Cloud Security

Cloud Resources

S3 Buckets	2
Azure Blobs	0
Google Storage	1
Firebase Apps	0
CloudFront	1
Publicly Exposed	No

Cloud Misconfigurations

Type	Service	Severity	Description
Missing Security Headers	CloudFront	Medium	CloudFront distribution is missing security headers: Content-Security-Policy, X-Frame-Options, X-XSS-Protection, X-Content-Type-Options

Vulnerabilities

Security Overview

Risk Score	High
Vulnerabilities	1
CVEs	0

Vulnerabilities

Name	Severity	Description	Remediation
Information Disclosure	High	Application exposes sensitive information through its API	Remove sensitive data from API responses

Email Credentials

Email Addresses

- info@soundcloud.com
- contact@soundcloud.com
- admin@soundcloud.com
- support@soundcloud.com
- sales@soundcloud.com
- help@soundcloud.com
- webmaster@soundcloud.com
- security@soundcloud.com

Exposed Data Types

Data Type	Count
Email Addresses	8
Passwords	0
Phone Numbers	0
Names	0
Addresses	0

Recommendations

- Address all critical and high severity vulnerabilities immediately
- Remove or restrict access to sensitive files exposed on the web server
- Implement API authentication mechanisms
- Restrict access to API documentation in production environments
- Remove sensitive information (API keys, tokens, etc.) from client-side JavaScript