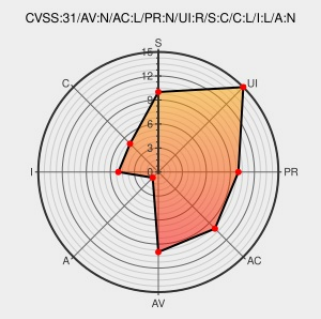
CVE-2019-8791

Published on: 12/18/2019 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:27:55 PM UTC

CVE-2019-8791

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF



Certain versions of Shazam from Apple contain the following vulnerability:

An issue existed in the parsing of URL schemes. This issue was addressed with improved URL validation. This issue is fixed in Shazam Android App Version 9.25.0, Shazam iOS App Version 12.11.0. Processing a maliciously crafted URL may lead to an open redirect.

CVE-2019-8791 has been assigned by product-security@apple.com to track the vulnerability - currently rated as MEDIUM severity.

Affected Vendor/Software: **Apple** - **Shazam-Android** version **< Shazam Android App Version 9.25.0**

Affected Vendor/Software: **Apple** - **Shazam-iOS** version **< Shazam iOS App Version 12.11.0**

CVSS3 Score: 6.1 - MEDIUM

Attack Vector	Attack Complexity	Privileges Required	User Interaction
NETWORK	LOW	NONE	REQUIRED
Scope	**Confidentiality Impact**	**Integrity Impact**	**Availability Impact**
CHANGED	LOW	LOW	NONE

CVSS2 Score: 5.8 - MEDIUM

Access Vector	Access Complexity	Authentication
NETWORK	MEDIUM	NONE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
PARTIAL	PARTIAL	NONE

CVE References

Description	Tags	Link

About the security content of Shazam Android App Version 9.25.0 - Apple Support	Vendor Advisory support.apple.com text/html	MISC support.apple.com/HT210744
Shazam iOS App バージョン 12.11.0 のセキュリティコンテンツについて - Apple サポート	Vendor Advisory support.apple.com text/html	MISC support.apple.com/HT210745

There are currently no QIDs associated with this CVE

Exploit/POC from Github

PoC for CVE-2019-8791 & CVE-2019-8792

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Apple	Shazam	All	All	All	All
Application	Apple	Shazam	All	All	All	All
Application	Apple	Shazam	All	All	All	All
Application	Apple	Shazam	All	All	All	All

cpe:2.3:a:apple:shazam:*:*:*:*:*:android:*:*:

cpe:2.3:a:apple:shazam:*:*:*:*:*:iphone_os:*:*:

cpe:2.3:a:apple:shazam:*:*:*:*:*:android:*:*:

cpe:2.3:a:apple:shazam:*:*:*:*:*:iphone_os:*:*:

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
@s3xcur1ty	How clicking a link can give away your precise location ash-king.co.uk/blog/Shazlocat… #InfoSec #CyberSecurity #Shazam	2021-08-11 17:14:17

← Previous ID

Next ID→

site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registred 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.

CVE.report and Source URL Uptime Status status.cve.report