

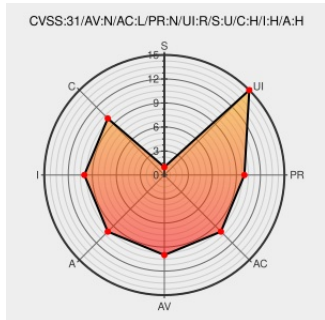


CVE-2019-8792

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

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

CVE-2019-8792

[Source: Mitre](#)[Source: NIST](#)[CVE.ORG](#)[Print: PDF](#) 

Certain versions of [Iphone Os](#) from [Apple](#) contain the following vulnerability:

An injection issue was addressed with improved 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 arbitrary javascript code execution.

CVE-2019-8792 has been assigned by product-security@apple.com to track the vulnerability - currently rated as **HIGH** 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: **8.8 - HIGH**

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

CVSS2 Score: **6.8 - MEDIUM**

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

CVE References

Description	Tags	Link
Apple - Shazam Android App - CVE-2019-8792 - HIGH	CVE-2019-8792	CVE-2019-8792

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

By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to comment@cve.report.

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
Operating System	Apple	Iphone Os	-	All	All	All
Operating System	Apple	Iphone Os	-	All	All	All
Application	Apple	Shazam	12.11.0	All	All	All
Application	Apple	Shazam	9.25.0	All	All	All
Application	Apple	Shazam	12.11.0	All	All	All
Application	Apple	Shazam	9.25.0	All	All	All
Operating System	Google	Android	-	All	All	All
Operating System	Google	Android	-	All	All	All

cpe:2.3:o:apple:iphone_os:-:*:*:*:*:*:

cpe:2.3:o:apple:iphone_os:-:*:*:*:*:*:

cpe:2.3:a:apple:shazam:12.11.0:*:*:*:*:*:

cpe:2.3:a:apple:shazam:9.25.0:*:*:*:*:*:

cpe:2.3:a:apple:shazam:12.11.0:*:*:*:*:*:

cpe:2.3:a:apple:shazam:9.25.0:*:*:*:*:*:

cpe:2.3:o:google:android:-:*:*:*:*:*:

cpe:2.3:o:google:android:-:*:*:*:*:*:

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
 @s3xcu1ty	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 →](#)

© [CVE.report](#) 2023   |

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](#).

CVE.report and Source URL Uptime Status [status.cve.report](#)