



CVE-2021-20748

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

Summary

CVE	CVE-2021-20748
State	PUBLIC
Assigner	vultures@jpcert.or.jp
Source Priority	CVE Program / NVD first with legacy fallback
Published	2021-07-14 02:15:00 UTC
Updated	2021-07-16 14:17:00 UTC
Description	Retty App for Android versions prior to 4.8.13 and Retty App for iOS versions prior to 4.11.14 uses a hard-coded API key fo

Risk And Classification

Problem Types: CWE-798

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Retty	Retty	All	All	All	All
Application	Retty	Retty	All	All	All	All

References

Reference	Source	Link
JVN#26891339: Multiple vulnerabilities in Retty App	MISC	jvn.jp
「Retty」のアプリで発生した不具合に関するお詫ひと対応完了に関するこゝろ報告_2.pdf - Google Drive	MISC	drive.google.co
CVE Program record	CVE.ORG	www.cve.org
NVD vulnerability detail	NVD	nvd.nist.gov

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

[630737](#) For Android Vulnerability CVE-2021-20748

[630771](#) For IOS Vulnerability CVE-2021-20748

© [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](#)