



CVE-2022-43543

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

Summary

CVE	CVE-2022-43543
State	PUBLIC
Assigner	vultures@jpcert.or.jp
Source Priority	CVE Program / NVD first with legacy fallback
Published	2022-12-21 09:15:00 UTC
Updated	2023-01-04 18:44:00 UTC
Description	KDDI +Message App, NTT DOCOMO +Message App, and SoftBank +Message App contain a vulnerability caused by impr

Risk And Classification

Problem Types: NVD-CWE-Other

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Docomo	Message	All	All	All	All
Application	Docomo	Message	All	All	All	All
Application	Kddi	Message	All	All	All	All
Application	Kddi	Message	All	All	All	All
Application	Softbank	Message	All	All	All	All
Application	Softbank	Message	All	All	All	All

References

Reference	Source	Link	Tags
+メッセージ (プラスメッセージ) スマートフォン・携帯電話 ソフトバンク	MISC	www.softbank.jp	
JVN#43561812: +Message App improper handling of Unicode control characters	MISC	jvn.jp	
お知らせ : +メッセージ (プラスメッセージ) サービス・機能 au	MISC	www.au.com	
+メッセージ (プラスメッセージ) サービス・機能 NTTドコモ	MISC	www.docomo.ne.jp	
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, analysis

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](#)