CVE-2013-3659

MITRE | NVD | CVE.ORG | JSON API | Print: PDF

Summary

CVE	CVE-2013-3659
State	PUBLISHED
Assigner	jpcert
Source Priority	CVE Program / NVD first with legacy fallback
Published	2013-08-09 19:55:07 UTC
Updated	2026-04-29 01:13:23 UTC
Description	The NTT DOCOMO overseas usage application 2.0.0 through 2.0.4 for Android does not properly connect to Wi-Fi access

Risk And Classification

Primary CVSS: v2.0 3.3 from nvd@nist.gov

AV:A/AC:L/Au:N/C:P/I:N/A:N

Problem Types: CWE-287 | n/a

CVSS v2.0 Breakdown

Access Vector

Adjacent

Access Complexity

Low

Authentication

None

Confidentiality

Partial

Integrity

None

Availability

None

AV:A/AC:L/Au:N/C:P/I:N/A:N

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Nttdocomo	Overseas Usage	2.0.0	All	All	All

Application	Nttdocomo	Overseas Usage	2.0.4	All	All	All

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Na	N/a	affected n/a	Not specified

References

Reference	Source	Li
JVN#44035194: docomo overseas usage application vulnerability in the connection process	af854a3a-2127-422b-91ae-364da2661108	jv
ドコモ海外利用 - Google Play'de Android Uygulamaları	af854a3a-2127-422b-91ae-364da2661108	pl
jvndb.jvn.jp/jvndb/JVNDB-2013-000075	af854a3a-2127-422b-91ae-364da2661108	jv
IBM X-Force Exchange	af854a3a-2127-422b-91ae-364da2661108	ex
Japan Vulnerability Notes/Information from NTT DOCOMO, INC.	af854a3a-2127-422b-91ae-364da2661108	jv
CVE Program record	CVE.ORG	w
NVD vulnerability detail	NVD	nv

No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.