CVE-2014-6024

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

Summary

CVE	CVE-2014-6024
State	PUBLISHED
Assigner	mitre
Source Priority	CVE Program / NVD first with legacy fallback
Published	2014-09-09 01:55:49 UTC
Updated	2026-05-06 22:30:45 UTC
Description	The Flurry library before 3.4.0 for Android does not verify X.509 certificates from SSL servers, which allows man-in-the-mid

Risk And Classification

Primary CVSS: v2.0 5.4 from nvd@nist.gov

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

Problem Types: CWE-310 | n/a

CVSS v2.0 Breakdown

Access Vector

Adjacent

Access Complexity

Medium

Authentication

None

Confidentiality

Partial

Integrity

Partial

Availability

Partial

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

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Flurry	Flurry-analytics-android	3.3.0	All	All	All

Application	Flurry	Flurry-analytics-android	3.3.2	All	All	All
Application	Flurry	Flurry-analytics-android	3.3.4	All	All	All

Vendor Declared Affected Products

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

References

Reference	Source
VU#582497 - Multiple Android applications fail to properly validate SSL certificates	af854a3a-2127-422b-91ae-364da266110
Android apps that fail to validate SSL - Google Sheets	af854a3a-2127-422b-91ae-364da266110
CERT Vulnerability Notes Database	af854a3a-2127-422b-91ae-364da266110
SSL Vulnerabilities: Who listens when Android applications talk? « Threat Research | FireEye Inc	af854a3a-2127-422b-91ae-364da266110
CVE Program record	CVE.ORG
NVD vulnerability detail	NVD

No vendor comments have been submitted for this CVE.

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