



CVE-2015-5666

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

Summary

CVE	CVE-2015-5666
State	PUBLIC
Assigner	vultures@jpcert.or.jp
Source Priority	CVE Program / NVD first with legacy fallback
Published	2017-09-25 21:29:00 UTC
Updated	2017-10-06 15:18:00 UTC
Description	ANA App for Android 3.1.1 and earlier, and ANA App for iOS 3.3.6 and earlier does not verify SSL certificates.

Risk And Classification

Problem Types: CWE-295

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Ana	All Nippon Airways	All	All	All	All
Application	Ana	All Nippon Airways	All	All	All	All

References

Reference	Source	Link	Tags
ANA App CVE-2015-5666 SSL Certificate Validation Security Bypass Vulnerability	BID	www.securityfocus.com	Third Party Advis
JVN#25086409: ANA App fails to verify SSL server certificates	JVN	jvn.jp	Third Party Advis
JVNDB-2015-000164 - JVN iPedia	JVNDB	jvndb.jvn.jp	Third Party Advis
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, analys

No vendor comments have been submitted for this CVE.

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

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