



CVE-2017-3190

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

Summary

CVE	CVE-2017-3190
State	PUBLIC
Assigner	cert@cert.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2017-12-16 02:29:00 UTC
Updated	2019-10-09 23:27:00 UTC
Description	Flash Seats Mobile App for Android version 1.7.9 and earlier and for iOS version 1.9.51 and earlier fails to properly validate

Risk And Classification

Problem Types: CWE-295

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Axs	Flash Seats	All	All	All	All
Application	Axs	Flash Seats	All	All	All	All

References

Reference	Source	Link	Tags
Flash Seats for iOS CVE-2017-3190 SSL Certificate Validation Security Bypass Vulnerability	BID	www.securityfocus.com	Third
Flash Seats Mobile App for iOS fails to validate SSL certificates Wilders Security Forums	MISC	www.wilderssecurity.com	Third
VU#247016 - Flash Seats Mobile App for Android and iOS fails to validate SSL certificates	CERT-VN	www.kb.cert.org	Third
CVE Program record	CVE.ORG	www.cve.org	canor
NVD vulnerability detail	NVD	nvd.nist.gov	canor

No vendor comments have been submitted for this CVE.

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

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