



CVE-2020-5526

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

Summary

CVE	CVE-2020-5526
State	PUBLIC
Assigner	vultures@jpcert.or.jp
Source Priority	CVE Program / NVD first with legacy fallback
Published	2020-01-31 04:15:00 UTC
Updated	2020-02-10 17:18:00 UTC
Description	The AWMS Mobile App for Android 2.0.0 to 2.0.5 and for iOS 2.0.0 to 2.0.8 does not verify X.509 certificates from servers,

Risk And Classification

Problem Types: CWE-295

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Fujixerox	Apeosware Management Suite	All	All	All	All
Application	Fujixerox	Apeosware Management Suite	All	All	All	All

References

Reference	Source	Link	Tags
Fuji Xerox Driver Download	MISC	onlinesupport.fujixerox.com	Vendor
JVN#00014057: AWMS Mobile App vulnerable to improper server certificate verification	MISC	jvn.jp	Third Pa
CVE Program record	CVE.ORG	www.cve.org	canonic
NVD vulnerability detail	NVD	nvd.nist.gov	canonic

No vendor comments have been submitted for this CVE.

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

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](#).

CVE.report and Source URL Uptime Status [status.cve.report](#)