



# CVE-2017-3160

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

## Summary

<b>CVE</b>	CVE-2017-3160
<b>State</b>	PUBLIC
<b>Assigner</b>	security@apache.org
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2018-02-01 21:29:00 UTC
<b>Updated</b>	2020-04-15 21:15:00 UTC
<b>Description</b>	After the Android platform is added to Cordova the first time, or after a project is created using the build scripts, the scripts v

## Risk And Classification

**Problem Types:** NVD-CWE-noinfo

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	<a href="#">Apache</a>	<a href="#">Cordova</a>	All	All	All	All
Application	<a href="#">Apache</a>	<a href="#">Cordova</a>	All	All	All	All

## References

Reference	Source	Link	Tags
Apache Cordova For Android CVE-2017-3160 Man in the Middle Security Bypass Vulnerability	BID	<a href="http://www.securityfocus.com">www.securityfocus.com</a>	Third
Apache Cordova Android 6.1.2 Released - Apache Cordova	MISC	<a href="http://cordova.apache.org">cordova.apache.org</a>	Mitiga
Oracle Critical Patch Update Advisory - April 2020	N/A	<a href="http://www.oracle.com">www.oracle.com</a>	
CVE Program record	CVE.ORG	<a href="http://www.cve.org">www.cve.org</a>	canon
NVD vulnerability detail	NVD	<a href="http://nvd.nist.gov">nvd.nist.gov</a>	canon

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](#)