



CVE-2019-0219

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

Summary

CVE	CVE-2019-0219
State	PUBLIC
Assigner	security@apache.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2020-01-14 15:15:00 UTC
Updated	2022-07-25 18:15:00 UTC
Description	A website running in the InAppBrowser webview on Android could execute arbitrary JavaScript in the main application's web

Risk And Classification

Problem Types: NVD-CWE-noinfo

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Apache	Cordova Inappbrowser	All	All	All	All
Application	Oracle	Instantis Enterprisetrack	17.1	All	All	All
Application	Oracle	Instantis Enterprisetrack	17.2	All	All	All
Application	Oracle	Instantis Enterprisetrack	17.3	All	All	All
Application	Oracle	Retail Xstore Point Of Service	16.0.6	All	All	All
Application	Oracle	Retail Xstore Point Of Service	17.0.4	All	All	All
Application	Oracle	Retail Xstore Point Of Service	18.0.3	All	All	All
Application	Oracle	Retail Xstore Point Of Service	19.0.2	All	All	All

References

Reference	Source	Link	Tags
Pony Mail!	MLIST	lists.apache.org	Vendor Ac
Oracle Critical Patch Update Advisory - July 2021	N/A	www.oracle.com	
lists.apache.org/thread/4vtg0trdrh5203dktt4f3vkd5z2d5ndj	MISC	lists.apache.org	
Oracle Critical Patch Update Advisory - July 2022	N/A	www.oracle.com	
Oracle Critical Patch Update Advisory - April 2021	MISC	www.oracle.com	
oss-security - CVE-2019-0219: Apache Cordova InAppBrowser Privilege Escalation (Android)	MLIST	www.openwall.com	Mailing Lis

CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical,

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

[983822](#) Nodejs (npm) Security Update for cordova-plugin-inappbrowser (GHSA-c6pw-q7f2-97hv)

© [CVE.report](https://cve.report) 2026 |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to 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](https://www.mitre.org) and the authoritative source of CVE content is [MITRE's CVE web site](https://www.mitre.org/cve). 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