



CVE-2017-5397

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

Summary

CVE	CVE-2017-5397
State	PUBLIC
Assigner	security@mozilla.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2018-06-11 21:29:00 UTC
Updated	2019-10-03 00:03:00 UTC
Description	The cache directory on the local file system is set to be world writable. Firefox defaults to extracting libraries from this cache

Risk And Classification

Problem Types: CWE-829

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Mozilla	Firefox	All	All	All	All
Application	Mozilla	Firefox	All	All	All	All

References

Reference	Source	Link	Tags
Mozilla Firefox for Android CVE-2017-5397 Security Bypass Vulnerability	BID	www.securityfocus.com	Third Party Advisory, VDB
Security vulnerabilities fixed in Firefox 51.0.3 — Mozilla	CONFIRM	www.mozilla.org	Vendor Advisory
1337304 - (CVE-2017-5397) Fennec cache directory is world writable	CONFIRM	bugzilla.mozilla.org	Issue Tracking, Patch, Ven
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, analysis

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