



CVE-2016-1948

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

Summary

CVE	CVE-2016-1948
State	PUBLIC
Assigner	security@mozilla.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2016-01-31 18:59:00 UTC
Updated	2017-09-10 01:29:00 UTC
Description	Mozilla Firefox before 44.0 on Android does not ensure that HTTPS is used for a lightweight-theme installation, which allow

Risk And Classification

Problem Types: CWE-310

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Google	Android	All	All	All	All
Operating System	Google	Android	All	All	All	All
Application	Mozilla	Firefox	43.0.4	All	All	All
Application	Mozilla	Firefox	43.0.4	All	All	All

References

Reference
Lightweight themes on Firefox for Android do not verify a secure connection — Mozilla
Mozilla Products: Multiple vulnerabilities (GLSA 201605-06) — Gentoo security
Mozilla Firefox Multiple Flaws Let Remote Users Execute Arbitrary Code, Spoof the Address Bar, Bypass Security Restrictions, and Deny Ser
1235876 - (CVE-2016-1948) LWT permissions exposed to man-in-the-middle attacks
CVE Program record
NVD vulnerability detail

No vendor comments have been submitted for this CVE.

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

© [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](#) 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](#)