



CVE-2015-2741

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

Summary

CVE	CVE-2015-2741
State	PUBLIC
Assigner	security@mozilla.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2015-07-06 02:01:00 UTC
Updated	2016-12-28 02:59:00 UTC
Description	Mozilla Firefox before 39.0, Firefox ESR 38.x before 38.1, and Thunderbird before 38.1 do not enforce key pinning upon en

Risk And Classification

Problem Types: CWE-310

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Mozilla	Firefox	All	All	All	All
Application	Mozilla	Firefox Esr	31.0	All	All	All
Application	Mozilla	Firefox Esr	31.1	All	All	All
Application	Mozilla	Firefox Esr	31.1.0	All	All	All
Application	Mozilla	Firefox Esr	31.1.1	All	All	All
Application	Mozilla	Firefox Esr	31.2	All	All	All
Application	Mozilla	Firefox Esr	31.3	All	All	All
Application	Mozilla	Firefox Esr	31.3.0	All	All	All
Application	Mozilla	Firefox Esr	31.4	All	All	All
Application	Mozilla	Firefox Esr	31.5	All	All	All
Application	Mozilla	Firefox Esr	31.5.1	All	All	All
Application	Mozilla	Firefox Esr	31.5.2	All	All	All
Application	Mozilla	Firefox Esr	31.5.3	All	All	All
Application	Mozilla	Firefox Esr	31.6.0	All	All	All
Application	Mozilla	Firefox Esr	31.7.0	All	All	All
Application	Mozilla	Firefox Esr	38.0	All	All	All
Application	Mozilla	Firefox Esr	31.0	All	All	All

Application	Mozilla	Firefox Esr	31.1	All	All	All
Application	Mozilla	Firefox Esr	31.1.0	All	All	All
Application	Mozilla	Firefox Esr	31.1.1	All	All	All
Application	Mozilla	Firefox Esr	31.2	All	All	All
Application	Mozilla	Firefox Esr	31.3	All	All	All
Application	Mozilla	Firefox Esr	31.3.0	All	All	All
Application	Mozilla	Firefox Esr	31.4	All	All	All
Application	Mozilla	Firefox Esr	31.5	All	All	All
Application	Mozilla	Firefox Esr	31.5.1	All	All	All
Application	Mozilla	Firefox Esr	31.5.2	All	All	All
Application	Mozilla	Firefox Esr	31.5.3	All	All	All
Application	Mozilla	Firefox Esr	31.6.0	All	All	All
Application	Mozilla	Firefox Esr	31.7.0	All	All	All
Application	Mozilla	Firefox Esr	38.0	All	All	All
Operating System	Oracle	Solaris	11.3	All	All	All
Operating System	Oracle	Solaris	11.3	All	All	All

References
Reference
Oracle Solaris Bulletin - April 2016
[security-announce] openSUSE-SU-2015:1229-1: important: Security update
Key pinning is ignored when overridable errors are encountered — Mozilla
Red Hat Customer Portal
Red Hat Customer Portal
USN-2656-2: Firefox vulnerabilities Ubuntu
1147497 – (CVE-2015-2741) key pinning checks for overridable errors do not work as intended by default
Mozilla Firefox Multiple Flaws Let Remote Users Execute Arbitrary Code, Obtain Potentially Sensitive Information, Bypass Security Restriction
Oracle Solaris Third Party Bulletin - October 2015
USN-2656-1: Firefox vulnerabilities Ubuntu
Mozilla Products: Multiple vulnerabilities (GLSA 201512-10) — Gentoo Security
Mozilla Thunderbird Multiple Flaws Let Remote Users Execute Arbitrary Code, Obtain Potentially Sensitive Information, and Bypass Security F
Mozilla Firefox/Thunderbird Multiple Security Vulnerabilities
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](#)