



CVE-2014-1480

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

Summary

CVE	CVE-2014-1480
State	PUBLIC
Assigner	security@mozilla.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2014-02-06 05:44:00 UTC
Updated	2020-08-21 18:40:00 UTC
Description	The file-download implementation in Mozilla Firefox before 27.0 and SeaMonkey before 2.24 does not properly restrict the t

Risk And Classification

Problem Types: CWE-1021

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Canonical	Ubuntu Linux	12.04	All	All	All
Operating System	Canonical	Ubuntu Linux	12.10	All	All	All
Operating System	Canonical	Ubuntu Linux	13.10	All	All	All
Operating System	Canonical	Ubuntu Linux	12.04	All	All	All
Operating System	Canonical	Ubuntu Linux	12.10	All	All	All
Operating System	Canonical	Ubuntu Linux	13.10	All	All	All
Application	Mozilla	Firefox	All	All	All	All
Application	Mozilla	Firefox	All	All	All	All
Application	Mozilla	Seamonkey	All	All	All	All
Application	Mozilla	Seamonkey	All	All	All	All
Operating System	Opensuse	Opensuse	11.4	All	All	All
Operating System	Opensuse	Opensuse	12.3	All	All	All
Operating System	Opensuse	Opensuse	13.1	All	All	All
Operating System	Opensuse	Opensuse	11.4	All	All	All
Operating System	Opensuse	Opensuse	12.3	All	All	All
Operating System	Opensuse	Opensuse	13.1	All	All	All
Operating System	Oracle	Solaris	11.3	All	All	All

Operating System	Oracle	Solaris	11.3	All	All	All
Operating System	Suse	Linux Enterprise Desktop	11	sp3	All	All
Operating System	Suse	Linux Enterprise Desktop	11	sp3	All	All
Operating System	Suse	Linux Enterprise Server	11	sp3	All	All
Operating System	Suse	Linux Enterprise Server	11	sp3	All	All
Operating System	Suse	Linux Enterprise Server	11	sp3	All	All
Operating System	Suse	Linux Enterprise Server	11	sp3	All	All
Operating System	Suse	Linux Enterprise Software Development Kit	11	sp3	All	All
Operating System	Suse	Linux Enterprise Software Development Kit	11	sp3	All	All

References

Reference

[Oracle Solaris Bulletin - April 2016](#)

[MFSA 2014-03: UI selection timeout missing on download prompts](#)

[\[security-announce\] openSUSE-SU-2014:0212-1: important: Mozilla Firefox](#)

[Mozilla Firefox/SeaMonkey CVE-2014-1480 Security Vulnerability](#)

[Gentoo Security](#)

[USN-2102-1: Firefox vulnerabilities | Ubuntu](#)

[Security Advisory SA56888 - Ubuntu update for firefox - Secunia](#)

[916726 – \(CVE-2014-1480\) Download "open file" dialog delay is too quick, doesn't prevent clickjacking](#)

[Mozilla Firefox Multiple Flaws Let Remote Users Execute Arbitrary Code and Obtain Potentially Sensitive Information - SecurityTracker](#)

[\[security-announce\] SUSE-SU-2014:0248-1: important: Security update for](#)

[IBM X-Force Exchange](#)

[USN-2102-2: Firefox regression | Ubuntu](#)

[102867](#)

[\[security-announce\] openSUSE-SU-2014:0419-1: important: Mozilla updates](#)

[Mozilla Seamonkey Multiple Bugs Let Remote Users Execute Arbitrary Code and Obtain Potentially Sensitive Information - SecurityTracker](#)

[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.

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](#).

CVE.report and Source URL Uptime Status [status.cve.report](#)