CVE-2014-1498

MITRE | NVD | CVE.ORG | Print: PDF

Summary

CVE	CVE-2014-1498
State	PUBLIC
Assigner	security@mozilla.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2014-03-19 10:55:00 UTC
Updated	2020-08-14 17:40:00 UTC
Description	The crypto.generateCRMFRequest method in Mozilla Firefox before 28.0 and SeaMonkey before 2.25 does not properly va

Risk And Classification

Problem Types: CWE-347

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
Application	Mozilla	Seamonkey	All	All	All	All
Application	Mozilla	Seamonkey	All	All	All	All
Operating System	Opensuse	Opensuse	13.1	All	All	All
Operating System	Opensuse	Opensuse	13.1	All	All	All
Operating System	Opensuse Project	Opensuse	11.4	All	All	All
Operating System	Opensuse Project	Opensuse	12.3	All	All	All
Operating System	Opensuse Project	Opensuse	11.4	All	All	All
Operating System	Opensuse Project	Opensuse	12.3	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	Source
Oracle Solaris Bulletin - April 2016	CONFIRM
935618 – (CVE-2014-1498) nsConvertToActualKeyGenParams uses the union in a SECKEYPublicKey without checking its type	CONFIRM
Gentoo Security	GENTOO
MFSA 2014-18: crypto.generateCRMFRequest does not validate type of key	CONFIRM
[security-announce] openSUSE-SU-2014:0584-1: important: MozillaThunderbi	SUSE
[security-announce] openSUSE-SU-2014:0448-1: important: MozillaFirefox:	SUSE
[security-announce] SUSE-SU-2014:0418-1: important: Security update for	SUSE
[security-announce] openSUSE-SU-2014:0419-1: important: Mozilla updates	SUSE
CVE Program record	CVE.ORG
NVD vulnerability detail	NVD

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 registred 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