



CVE-2010-2198

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

Summary

CVE	CVE-2010-2198
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2010-06-08 18:30:00 UTC
Updated	2023-11-07 02:05:00 UTC
Description	lib/fsm.c in RPM 4.8.0 and earlier does not properly reset the metadata of an executable file during replacement of the file in

Risk And Classification

Problem Types: CWE-264

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Rpm	Rpm	1.2	All	All	All
Application	Rpm	Rpm	1.3	All	All	All
Application	Rpm	Rpm	1.3.1	All	All	All
Application	Rpm	Rpm	1.4	All	All	All
Application	Rpm	Rpm	1.4.2	All	All	All
Application	Rpm	Rpm	1.4.2/a	All	All	All
Application	Rpm	Rpm	1.4.2Va	All	All	All
Application	Rpm	Rpm	1.4.3	All	All	All
Application	Rpm	Rpm	1.4.4	All	All	All
Application	Rpm	Rpm	1.4.5	All	All	All
Application	Rpm	Rpm	1.4.6	All	All	All
Application	Rpm	Rpm	1.4.7	All	All	All
Application	Rpm	Rpm	2..4.10	All	All	All
Application	Rpm	Rpm	2.0	All	All	All
Application	Rpm	Rpm	2.0.1	All	All	All
Application	Rpm	Rpm	2.0.10	All	All	All
Application	Rpm	Rpm	2.0.11	All	All	All

Application	Rpm	Rpm	2.0.2	All	All	All
Application	Rpm	Rpm	2.0.3	All	All	All
Application	Rpm	Rpm	2.0.4	All	All	All
Application	Rpm	Rpm	2.0.5	All	All	All
Application	Rpm	Rpm	2.0.6	All	All	All
Application	Rpm	Rpm	2.0.7	All	All	All
Application	Rpm	Rpm	2.0.8	All	All	All
Application	Rpm	Rpm	2.0.9	All	All	All
Application	Rpm	Rpm	2.1	All	All	All
Application	Rpm	Rpm	2.1.1	All	All	All
Application	Rpm	Rpm	2.1.2	All	All	All
Application	Rpm	Rpm	2.2	All	All	All
Application	Rpm	Rpm	2.2.1	All	All	All
Application	Rpm	Rpm	2.2.10	All	All	All
Application	Rpm	Rpm	2.2.11	All	All	All
Application	Rpm	Rpm	2.2.2	All	All	All
Application	Rpm	Rpm	2.2.3	All	All	All
Application	Rpm	Rpm	2.2.3.10	All	All	All
Application	Rpm	Rpm	2.2.3.11	All	All	All
Application	Rpm	Rpm	2.2.4	All	All	All
Application	Rpm	Rpm	2.2.5	All	All	All
Application	Rpm	Rpm	2.2.6	All	All	All
Application	Rpm	Rpm	2.2.7	All	All	All
Application	Rpm	Rpm	2.2.8	All	All	All
Application	Rpm	Rpm	2.2.9	All	All	All
Application	Rpm	Rpm	2.3	All	All	All
Application	Rpm	Rpm	2.3.1	All	All	All
Application	Rpm	Rpm	2.3.2	All	All	All
Application	Rpm	Rpm	2.3.3	All	All	All
Application	Rpm	Rpm	2.3.4	All	All	All
Application	Rpm	Rpm	2.3.5	All	All	All
Application	Rpm	Rpm	2.3.6	All	All	All
Application	Rpm	Rpm	2.3.7	All	All	All
Application	Rpm	Rpm	2.3.8	All	All	All
Application	Rpm	Rpm	2.3.9	All	All	All

Application	Rpm	Rpm	2.4.1	All	All	All
Application	Rpm	Rpm	2.4.11	All	All	All
Application	Rpm	Rpm	2.4.12	All	All	All
Application	Rpm	Rpm	2.4.2	All	All	All
Application	Rpm	Rpm	2.4.3	All	All	All
Application	Rpm	Rpm	2.4.4	All	All	All
Application	Rpm	Rpm	2.4.5	All	All	All
Application	Rpm	Rpm	2.4.6	All	All	All
Application	Rpm	Rpm	2.4.8	All	All	All
Application	Rpm	Rpm	2.4.9	All	All	All
Application	Rpm	Rpm	2.5	All	All	All
Application	Rpm	Rpm	2.5.1	All	All	All
Application	Rpm	Rpm	2.5.2	All	All	All
Application	Rpm	Rpm	2.5.3	All	All	All
Application	Rpm	Rpm	2.5.4	All	All	All
Application	Rpm	Rpm	2.5.5	All	All	All
Application	Rpm	Rpm	2.5.6	All	All	All
Application	Rpm	Rpm	2.6.7	All	All	All
Application	Rpm	Rpm	3.0	All	All	All
Application	Rpm	Rpm	3.0.1	All	All	All
Application	Rpm	Rpm	3.0.2	All	All	All
Application	Rpm	Rpm	3.0.3	All	All	All
Application	Rpm	Rpm	3.0.4	All	All	All
Application	Rpm	Rpm	3.0.5	All	All	All
Application	Rpm	Rpm	3.0.6	All	All	All
Application	Rpm	Rpm	4.0.	All	All	All
Application	Rpm	Rpm	4.0.1	All	All	All
Application	Rpm	Rpm	4.0.2	All	All	All
Application	Rpm	Rpm	4.0.3	All	All	All
Application	Rpm	Rpm	4.0.4	All	All	All
Application	Rpm	Rpm	4.1	All	All	All
Application	Rpm	Rpm	4.3.3	All	All	All
Application	Rpm	Rpm	4.4.2	All	All	All
Application	Rpm	Rpm	4.4.2.1	All	All	All
Application	Rpm	Rpm	4.4.2.2	All	All	All
Application	Rpm	Rpm	4.4.2.3	All	All	All

Application	Rpm	Rpm	4.4.2.3	All	All	All
Application	Rpm	Rpm	4.6.0	All	All	All
Application	Rpm	Rpm	4.6.1	All	All	All
Application	Rpm	Rpm	4.7.0	All	All	All
Application	Rpm	Rpm	4.7.1	All	All	All
Application	Rpm	Rpm	4.7.2	All	All	All
Application	Rpm	Rpm	1.2	All	All	All
Application	Rpm	Rpm	1.3	All	All	All
Application	Rpm	Rpm	1.3.1	All	All	All
Application	Rpm	Rpm	1.4	All	All	All
Application	Rpm	Rpm	1.4.2	All	All	All
Application	Rpm	Rpm	1.4.2Va	All	All	All
Application	Rpm	Rpm	1.4.3	All	All	All
Application	Rpm	Rpm	1.4.4	All	All	All
Application	Rpm	Rpm	1.4.5	All	All	All
Application	Rpm	Rpm	1.4.6	All	All	All
Application	Rpm	Rpm	1.4.7	All	All	All
Application	Rpm	Rpm	2..4.10	All	All	All
Application	Rpm	Rpm	2.0	All	All	All
Application	Rpm	Rpm	2.0.1	All	All	All
Application	Rpm	Rpm	2.0.10	All	All	All
Application	Rpm	Rpm	2.0.11	All	All	All
Application	Rpm	Rpm	2.0.2	All	All	All
Application	Rpm	Rpm	2.0.3	All	All	All
Application	Rpm	Rpm	2.0.4	All	All	All
Application	Rpm	Rpm	2.0.5	All	All	All
Application	Rpm	Rpm	2.0.6	All	All	All
Application	Rpm	Rpm	2.0.7	All	All	All
Application	Rpm	Rpm	2.0.8	All	All	All
Application	Rpm	Rpm	2.0.9	All	All	All
Application	Rpm	Rpm	2.1	All	All	All
Application	Rpm	Rpm	2.1.1	All	All	All
Application	Rpm	Rpm	2.1.2	All	All	All
Application	Rpm	Rpm	2.2	All	All	All
Application	Rpm	Rpm	2.2.1	All	All	All
Application	Rpm	Rpm	2.2.10	All	All	All

Application	Rpm	Rpm	2.2.11	All	All	All
Application	Rpm	Rpm	2.2.2	All	All	All
Application	Rpm	Rpm	2.2.3	All	All	All
Application	Rpm	Rpm	2.2.3.10	All	All	All
Application	Rpm	Rpm	2.2.3.11	All	All	All
Application	Rpm	Rpm	2.2.4	All	All	All
Application	Rpm	Rpm	2.2.5	All	All	All
Application	Rpm	Rpm	2.2.6	All	All	All
Application	Rpm	Rpm	2.2.7	All	All	All
Application	Rpm	Rpm	2.2.8	All	All	All
Application	Rpm	Rpm	2.2.9	All	All	All
Application	Rpm	Rpm	2.3	All	All	All
Application	Rpm	Rpm	2.3.1	All	All	All
Application	Rpm	Rpm	2.3.2	All	All	All
Application	Rpm	Rpm	2.3.3	All	All	All
Application	Rpm	Rpm	2.3.4	All	All	All
Application	Rpm	Rpm	2.3.5	All	All	All
Application	Rpm	Rpm	2.3.6	All	All	All
Application	Rpm	Rpm	2.3.7	All	All	All
Application	Rpm	Rpm	2.3.8	All	All	All
Application	Rpm	Rpm	2.3.9	All	All	All
Application	Rpm	Rpm	2.4.1	All	All	All
Application	Rpm	Rpm	2.4.11	All	All	All
Application	Rpm	Rpm	2.4.12	All	All	All
Application	Rpm	Rpm	2.4.2	All	All	All
Application	Rpm	Rpm	2.4.3	All	All	All
Application	Rpm	Rpm	2.4.4	All	All	All
Application	Rpm	Rpm	2.4.5	All	All	All
Application	Rpm	Rpm	2.4.6	All	All	All
Application	Rpm	Rpm	2.4.8	All	All	All
Application	Rpm	Rpm	2.4.9	All	All	All
Application	Rpm	Rpm	2.5	All	All	All
Application	Rpm	Rpm	2.5.1	All	All	All
Application	Rpm	Rpm	2.5.2	All	All	All
Application	Rpm	Rpm	2.5.3	All	All	All

Application	Rpm	Rpm	2.5.4	All	All	All
Application	Rpm	Rpm	2.5.5	All	All	All
Application	Rpm	Rpm	2.5.6	All	All	All
Application	Rpm	Rpm	2.6.7	All	All	All
Application	Rpm	Rpm	3.0	All	All	All
Application	Rpm	Rpm	3.0.1	All	All	All
Application	Rpm	Rpm	3.0.2	All	All	All
Application	Rpm	Rpm	3.0.3	All	All	All
Application	Rpm	Rpm	3.0.4	All	All	All
Application	Rpm	Rpm	3.0.5	All	All	All
Application	Rpm	Rpm	3.0.6	All	All	All
Application	Rpm	Rpm	4.0.	All	All	All
Application	Rpm	Rpm	4.0.1	All	All	All
Application	Rpm	Rpm	4.0.2	All	All	All
Application	Rpm	Rpm	4.0.3	All	All	All
Application	Rpm	Rpm	4.0.4	All	All	All
Application	Rpm	Rpm	4.1	All	All	All
Application	Rpm	Rpm	4.3.3	All	All	All
Application	Rpm	Rpm	4.4.2	All	All	All
Application	Rpm	Rpm	4.4.2.1	All	All	All
Application	Rpm	Rpm	4.4.2.2	All	All	All
Application	Rpm	Rpm	4.4.2.3	All	All	All
Application	Rpm	Rpm	4.6.0	All	All	All
Application	Rpm	Rpm	4.6.1	All	All	All
Application	Rpm	Rpm	4.7.0	All	All	All
Application	Rpm	Rpm	4.7.1	All	All	All
Application	Rpm	Rpm	4.7.2	All	All	All
Application	Rpm	Rpm	All	All	All	All

References						
Reference					Source	Link
'Re: [oss-security] CVE Request -- rpm -- Fails to remove the' - MARC					MLIST	marc.info
oss-security - Re: CVE Request -- rpm -- Fails to remove the SUID/SGID bits on package upgrade (RH BZ#598775)					MLIST	www.ope
65144					OSVDB	www.osv
rpm.org Git Repositories - rpm.git/commit						rpm.org
oss-security - Re: CVE Request -- rpm -- Fails to remove the SUID/SGID bits on package upgrade (RH BZ#598775)					MLIST	www.ope

Bug 598775 – CVE-2010-2059 rpm: fails to drop SUID/SGID bits on package upgrade	CONFIRM	bugzilla.r
rpm.org Git Repositories - rpm.git/commit	CONFIRM	rpm.org
RPM Package Manager Package Upgrade File Metadata Update Weaknesses - Advisories - Community	SECUNIA	secunia.c
oss-security - Re: CVE Request -- rpm -- Fails to remove the SUID/SGID bits on package upgrade (RH BZ#598775)	MLIST	www.ope
CVE Program record	CVE.ORG	www.cve
NVD vulnerability detail	NVD	nvd.nist.g

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](#).

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