



CVE-2013-6435

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

Summary

CVE	CVE-2013-6435
State	PUBLIC
Assigner	secalert@redhat.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2014-12-16 18:59:00 UTC
Updated	2023-02-13 00:29:00 UTC
Description	Race condition in RPM 4.11.1 and earlier allows remote attackers to execute arbitrary code via a crafted RPM file whose in

Risk And Classification

Problem Types: CWE-74

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Debian	Debian Linux	7.0	All	All	All
Operating System	Debian	Debian Linux	7.0	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	1.4.1	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	1.4.2/a	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	2.0	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	4.10.2	All	All	All
Application	Rpm	Rpm	4.3.3	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	4.5.90	All	All	All
Application	Rpm	Rpm	4.6.0	All	All	All
Application	Rpm	Rpm	4.6.0	rc1	All	All
Application	Rpm	Rpm	4.6.0	rc2	All	All
Application	Rpm	Rpm	4.6.0	rc3	All	All
Application	Rpm	Rpm	4.6.0	rc4	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	4.8.0	All	All	All
Application	Rpm	Rpm	4.8.1	All	All	All
Application	Rpm	Rpm	4.9.0	All	All	All
Application	Rpm	Rpm	4.9.0	alpha	All	All
Application	Rpm	Rpm	4.9.0	beta1	All	All
Application	Rpm	Rpm	4.9.0	rc1	All	All
Application	Rpm	Rpm	4.9.1	All	All	All
Application	Rpm	Rpm	4.9.1.1	All	All	All
Application	Rpm	Rpm	4.9.1.2	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	1.4.1	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	2.0	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	4.10.0	All	All	All

Application	Rpm	Rpm	4.10.0	All	All	All
Application	Rpm	Rpm	4.10.1	All	All	All
Application	Rpm	Rpm	4.10.2	All	All	All
Application	Rpm	Rpm	4.3.3	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	4.5.90	All	All	All
Application	Rpm	Rpm	4.6.0	All	All	All
Application	Rpm	Rpm	4.6.0	rc1	All	All
Application	Rpm	Rpm	4.6.0	rc2	All	All
Application	Rpm	Rpm	4.6.0	rc3	All	All
Application	Rpm	Rpm	4.6.0	rc4	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	4.8.0	All	All	All
Application	Rpm	Rpm	4.8.1	All	All	All
Application	Rpm	Rpm	4.9.0	All	All	All
Application	Rpm	Rpm	4.9.0	alpha	All	All
Application	Rpm	Rpm	4.9.0	beta1	All	All
Application	Rpm	Rpm	4.9.0	rc1	All	All
Application	Rpm	Rpm	4.9.1	All	All	All
Application	Rpm	Rpm	4.9.1.1	All	All	All
Application	Rpm	Rpm	4.9.1.2	All	All	All
Application	Rpm	Rpm	All	All	All	All

References

Reference	Source	Link	Tags
Red Hat Customer Portal	REDHAT	rhn.redhat.com	
Red Hat Customer Portal	MISC	access.redhat.com	
Red Hat Customer Portal	REDHAT	rhn.redhat.com	
Red Hat Customer Portal	MISC	access.redhat.com	
RPM: Multiple vulnerabilities (GLSA 201811-22) — Gentoo security	GENTOO	security.gentoo.org	
Red Hat Customer Portal	MISC	access.redhat.com	

Bug 1039811 – CVE-2013-6435 rpm: race condition during the installation process	CONFIRM	bugzilla.redhat.com	
Oracle VM Server for x86 Bulletin - July 2016	CONFIRM	www.oracle.com	
Support / Security / Advisories // MDVSA-2015:056 Mandriva	MANDRIVA	www.mandriva.com	
RPM CVE-2013-6435 Remote Code Execution Vulnerability	BID	www.securityfocus.com	
Debian -- Security Information -- DSA-3129-1 rpm	DEBIAN	www.debian.org	
access.redhat.com CVE-2013-6435	MISC	access.redhat.com	
Red Hat Customer Portal	REDHAT	rhn.redhat.com	
Analysis of the CVE-2013-6435 Flaw in RPM Red Hat Security	CONFIRM	securityblog.redhat.com	
Support / Security / Advisories // MDVSA-2014:251 Mandriva	MANDRIVA	www.mandriva.com	
Juniper Networks - 2015-10 Security Bulletin: CTPView: Multiple Vulnerabilities in CTPView	CONFIRM	kb.juniper.net	
Mageia Advisory: MGASA-2014-0529 - Updated rpm packages fix security vulnerabilities	CONFIRM	advisories.mageia.org	
CVE Program record	CVE.ORG	www.cve.org	canon
NVD vulnerability detail	NVD	nvd.nist.gov	canon

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

[710222](#) Gentoo Linux RPM Multiple Vulnerabilities (GLSA 201811-22)

© 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