



CVE-2011-0714

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

Summary

CVE	CVE-2011-0714
State	PUBLIC
Assigner	secalert@redhat.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2011-05-04 22:55:00 UTC
Updated	2019-04-22 17:48:00 UTC
Description	Use-after-free vulnerability in a certain Red Hat patch for the RPC server sockets functionality in the Linux kernel 2.6.32 on

Risk And Classification

Problem Types: CWE-399

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Linux	Linux Kernel	2.6.32	All	All	All
Operating System	Linux	Linux Kernel	2.6.32	All	All	All
Operating System	Redhat	Enterprise Linux	6.0	All	All	All
Operating System	Redhat	Enterprise Linux	6.0	All	All	All

References

Reference	Source	Link	Tags
Bug 678144 – CVE-2011-0714 kernel: deficiency in handling of invalid data packets in lockd	CONFIRM	bugzilla.redhat.com	
oss-security - CVE-2011-0714 kernel: deficiency in handling of invalid data packets in lockd	MLIST	openwall.com	
access.redhat.com	REDHAT	rhn.redhat.com	Vendor
oss-security - Re: CVE-2011-0714 kernel: deficiency in handling of invalid data packets in lockd	MLIST	openwall.com	
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical

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](#)