



CVE-2012-6704

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

Summary

CVE	CVE-2012-6704
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2016-12-28 07:59:00 UTC
Updated	2023-01-17 21:45:00 UTC
Description	The sock_setsockopt function in net/core/sock.c in the Linux kernel before 3.5 mishandles negative values of sk_sndbuf an

Risk And Classification

Problem Types: CWE-119

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Linux	Linux Kernel	All	All	All	All
Operating System	Linux	Linux Kernel	All	All	All	All

References

Reference	Source	Link
oss-security - Re: CVE Request: Linux: signed overflows for SO_{SND RCV}BUFFORCE	MLIST	www.openwall.com
Bug 1402024 – CVE-2012-6704 kernel: Signed overflows in SO_{SND RCV}BUF in sock_setsockopt()	CONFIRM	bugzilla.redhat.com
net: cleanups in sock_setsockopt() · torvalds/linux@8298193 · GitHub	CONFIRM	github.com
Linux Kernel CVE-2012-6704 Local Denial of Service Vulnerability	BID	www.securityfocus.com
kernel/git/torvalds/linux.git - Linux kernel source tree	CONFIRM	git.kernel.org
CVE Program record	CVE.ORG	www.cve.org
NVD vulnerability detail	NVD	nvd.nist.gov

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](#)