



CVE-2012-6689

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

Summary

CVE	CVE-2012-6689
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2016-05-02 10:59:00 UTC
Updated	2023-01-20 14:30:00 UTC
Description	The netlink_sendmsg function in net/netlink/af_netlink.c in the Linux kernel before 3.5.5 does not validate the dst_pid field, v

Risk And Classification

Problem Types: CWE-284

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
kernel/git/torvalds/linux.git - Linux kernel source tree
'[PATCH 0/2] netlink patches' - MARC
libmnl 'mnl_nlmsg_portid_ok()' Function Local Security Bypass Vulnerability
www.kernel.org/pub/linux/kernel/v3.x/ChangeLog-3.5.5
netlink: fix possible spoofing from non-root processes · torvalds/linux@20e1db1 · GitHub
'[PATCH 2/2] [RFC] netlink: fix possible spoofing from non-root processes' - MARC
oss-security - Re: libmnl: incorrect validation of netlink message origin allows attackers to spoof netlink messages
848949 – (CVE-2012-6689) CVE-2012-6689 libmnl: incorrect validation of netlink message origin allows attackers to spoof netlink messages
CVE Program record
NVD vulnerability detail

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](#)