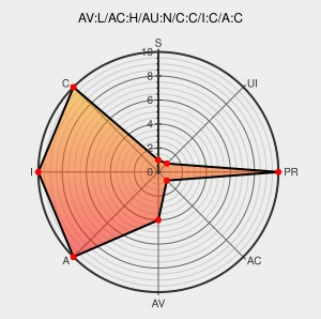
CVE-2013-1827

Published on: 03/22/2013 12:00:00 AM UTC

Last Modified on: 02/13/2023 04:41:00 AM UTC

CVE-2013-1827

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF



Certain versions of Linux Kernel from Linux contain the following vulnerability:

net/dccp/ccid.h in the Linux kernel before 3.5.4 allows local users to gain privileges or cause a denial of service (NULL pointer dereference and system crash) by leveraging the CAP_NET_ADMIN capability for a certain (1) sender or (2) receiver getsockopt call.

CVE-2013-1827 has been assigned by secalert@redhat.com to track the vulnerability

CVSS2 Score: 6.2 - MEDIUM

Access Vector	Access Complexity	Authentication
LOCAL	HIGH	NONE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
COMPLETE	COMPLETE	COMPLETE

CVE References

Description	Tags	Link
kernel/git/torvalds/linux.git - Linux kernel source tree	Exploit, Patch, web.archive.org, text/html, Inactive Link, Not Archived	MISC git.kernel.org/?p=linux/kernel/git/torvalds/linux-2.6.git%3Ba=commit%3Bh=276bdb82dedb290511467a5a4fdbe9f0b52dce6f
919164 – (CVE-2013-1827) CVE-2013-1827 Kernel: dccp: check ccid before NULL poiter dereference	bugzilla.redhat.com, text/html	CONFIRM bugzilla.redhat.com/show_bug.cgi?id=919164
Red Hat Customer Portal	web.archive.org, text/html, Inactive Link, Not Archived	REDHAT RHSA-2013:0744
	www.kernel.org	CONFIRM www.kernel.org/pub/linux/kernel/v3.x/ChangeLog-3.5.4

	text/plain	
oss-security - Re: CVE Requests (maybe): Linux kernel: various info leaks, some NULL ptr derefs	www.openwall.com text/html	MLIST [oss-security] 20130307 Re: CVE Requests (maybe): Linux kernel: various info leaks, some NULL ptr derefs
dccp: check ccid before dereferencing · torvalds/linux@276bdb8 · GitHub	Exploit Patch github.com text/html	CONFIRM github.com/torvalds/linux/commit/276bdb82dedb290511467a5a4fdbe9f0b52dce6f

By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to comment@cve.report.

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Linux	Linux Kernel	3.5.1	All	All	All
Operating System	Linux	Linux Kernel	3.5.2	All	All	All
Operating System	Linux	Linux Kernel	3.5.1	All	All	All
Operating System	Linux	Linux Kernel	3.5.2	All	All	All
Operating System	Linux	Linux Kernel	All	All	All	All

cpe:2.3:o:linux:linux_kernel:3.5.1:*:*:*:*:*:*:*:

cpe:2.3:o:linux:linux_kernel:3.5.2:*:*:*:*:*:*:*:

cpe:2.3:o:linux:linux_kernel:3.5.1:*:*:*:*:*:*:*:

cpe:2.3:o:linux:linux_kernel:3.5.2:*:*:*:*:*:*:*:

cpe:2.3:o:linux:linux_kernel:*:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→

© CVE.report 2023 | 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 registred 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