



CVE-2009-3288

Published on: 09/22/2009 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:25:24 PM UTC

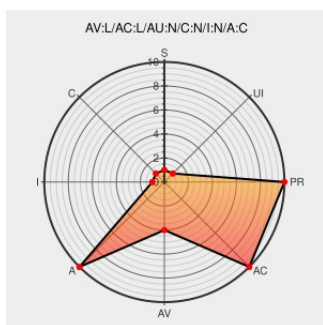
CVE-2009-3288

Source: Mitre

Source: NIST

CVE.ORG

Print: PDF



Certain versions of [Linux Kernel](#) from [Kernel](#) contain the following vulnerability:

The `sg_build_indirect` function in `drivers/scsi/sg.c` in Linux kernel 2.6.28-rc1 through 2.6.31-rc8 uses an incorrect variable when accessing an array, which allows local users to cause a denial of service (kernel OOPS and NULL pointer dereference), as demonstrated by using `xcdroast` to duplicate a CD. NOTE: this is only exploitable by users who can open the cdrom device.

CVE-2009-3288 has been assigned by [M](#) cve@mitre.org to track the vulnerability

CVSS2 Score: **4.9 - MEDIUM**

Access Vector

Access Complexity

Authentication

LOCAL

LOW

NONE

Confidentiality Impact

Integrity Impact

Availability Impact

NONE

NONE

COMPLETE

CVE References

Description

Tags

Link

LKML: Bob Tracy: [BUG] 2.6.31-rc8 readcd Oops

Exploit
lkml.org
text/xml

[LKML](#) [MLIST \[linux-kernel\] 20090902 \[BUG\] 2.6.31-rc8 readcd Oops](#)

LKML: Michal Schmidt: [PATCH] sg: fix oops in the error path in `sg_build_indirect()`

Exploit
lkml.org
text/xml

[LKML](#) [MLIST \[linux-kernel\] 20090903 \[PATCH\] sg: fix oops in the error path in `sg\_build\_indirect\(\)`](#)

oss-security - CVE request: kernel: NULL pointer dereference in `sg_build_indirect()`

Exploit
www.openwall.com
text/html

[OSS](#) [MLIST \[oss-security\] 20090904 CVE request: kernel: NULL pointer dereference in `sg\_build\_indirect\(\)`](#)

Ubuntu update for kernel - Secunia Advisories - Vulnerability Information - Secunia.com

web.archive.org
text/html

[SECUNIA](#) 37105

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
Application	Kernel	Linux Kernel	2.6.28-rc1	All	All	All
Application	Kernel	Linux Kernel	2.6.28-rc1	All	All	All
Operating System	Linux	Linux Kernel	2.6.31-rc10	All	All	All
Operating System	Linux	Linux Kernel	2.6.31-rc2	All	All	All
Operating System	Linux	Linux Kernel	2.6.31-rc3	All	All	All
Operating System	Linux	Linux Kernel	2.6.31-rc4	All	All	All
Operating System	Linux	Linux Kernel	2.6.31-rc5	All	All	All
Operating System	Linux	Linux Kernel	2.6.31-rc6	All	All	All
Operating System	Linux	Linux Kernel	2.6.31-rc7	All	All	All
Operating System	Linux	Linux Kernel	2.6.31-rc8	All	All	All
Operating System	Linux	Linux Kernel	2.6.31-rc9	All	All	All
Operating System	Linux	Linux Kernel	2.6.31-rc10	All	All	All
Operating System	Linux	Linux Kernel	2.6.31-rc2	All	All	All
Operating System	Linux	Linux Kernel	2.6.31-rc3	All	All	All
Operating System	Linux	Linux Kernel	2.6.31-rc4	All	All	All
Operating System	Linux	Linux Kernel	2.6.31-rc5	All	All	All
Operating System	Linux	Linux Kernel	2.6.31-rc6	All	All	All
Operating System	Linux	Linux Kernel	2.6.31-rc7	All	All	All

Operating System	Linux	Linux Kernel	2.6.31-rc7	All	All	All
Operating System	Linux	Linux Kernel	2.6.31-rc8	All	All	All
Operating System	Linux	Linux Kernel	2.6.31-rc9	All	All	All
cpe:2.3:a:kernel:linux_kernel:2.6.28-rc1:*****:						
cpe:2.3:a:kernel:linux_kernel:2.6.28-rc1:*****:						
cpe:2.3:o:linux:linux_kernel:2.6.31-rc10:*****:						
cpe:2.3:o:linux:linux_kernel:2.6.31-rc2:*****:						
cpe:2.3:o:linux:linux_kernel:2.6.31-rc3:*****:						
cpe:2.3:o:linux:linux_kernel:2.6.31-rc4:*****:						
cpe:2.3:o:linux:linux_kernel:2.6.31-rc5:*****:						
cpe:2.3:o:linux:linux_kernel:2.6.31-rc6:*****:						
cpe:2.3:o:linux:linux_kernel:2.6.31-rc7:*****:						
cpe:2.3:o:linux:linux_kernel:2.6.31-rc8:*****:						
cpe:2.3:o:linux:linux_kernel:2.6.31-rc9:*****:						
cpe:2.3:o:linux:linux_kernel:2.6.31-rc10:*****:						
cpe:2.3:o:linux:linux_kernel:2.6.31-rc2:*****:						
cpe:2.3:o:linux:linux_kernel:2.6.31-rc3:*****:						
cpe:2.3:o:linux:linux_kernel:2.6.31-rc4:*****:						
cpe:2.3:o:linux:linux_kernel:2.6.31-rc5:*****:						
cpe:2.3:o:linux:linux_kernel:2.6.31-rc6:*****:						
cpe:2.3:o:linux:linux_kernel:2.6.31-rc7:*****:						
cpe:2.3:o:linux:linux_kernel:2.6.31-rc8:*****:						
cpe:2.3:o:linux:linux_kernel:2.6.31-rc9:*****:						

[← Previous ID](#)

[Next ID →](#)

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](#)