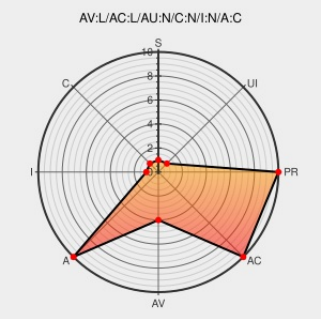
CVE-2011-1023

Published on: 06/21/2012 12:00:00 AM UTC

Last Modified on: 02/13/2023 01:18:00 AM UTC

CVE-2011-1023

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



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

The Reliable Datagram Sockets (RDS) subsystem in the Linux kernel before 2.6.38 does not properly handle congestion map updates, which allows local users to cause a denial of service (BUG_ON and system crash) via vectors involving (1) a loopback (aka loop) transmit operation or (2) an InfiniBand (aka ib) transmit operation.

CVE-2011-1023 has been assigned by secalert@redhat.com 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
kernel/git/torvalds/linux.git - Linux kernel source tree	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=6094628bfd94323fc1cea05ec2c6affd98c18f7f
404 Not Found	ftp.osuosl.org text/html Inactive Link Not Archived	CONFIRM ftp.osuosl.org/pub/linux/kernel/v2.6/ChangeLog-2.6.38
oss-security - CVE-2011-1023 kernel: rds: prevent BUG_ON triggering on congestion map updates	www.openwall.com text/html	MLIST [oss-security] 20110303 CVE-2011-1023 kernel: rds: prevent BUG_ON triggering on congestion map updates
680345 – (CVE-2011-1023) CVE-2011-1023 kernel:	bugzilla.redhat.com text/html	CONFIRM bugzilla.redhat.com/show_bug.cgi?id=680345

BUG_ON() in rds_send_xmit()

rds: prevent BUG_ON triggering on congestion map updates · torvalds/linux@6094628 · GitHub	Exploit Patch github.com text/html	CONFIRM github.com/torvalds/linux/commit/6094628bfd94323fc1cea05ec2c6affd98c18f7f

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	2.6.37	All	All	All
Operating System	Linux	Linux Kernel	2.6.37	rc1	All	All
Operating System	Linux	Linux Kernel	2.6.37	rc2	All	All
Operating System	Linux	Linux Kernel	2.6.37	rc3	All	All
Operating System	Linux	Linux Kernel	2.6.37	rc4	All	All
Operating System	Linux	Linux Kernel	2.6.37	rc5	All	All
Operating System	Linux	Linux Kernel	2.6.37.1	All	All	All
Operating System	Linux	Linux Kernel	2.6.37.2	All	All	All
Operating System	Linux	Linux Kernel	2.6.37.3	All	All	All
Operating System	Linux	Linux Kernel	2.6.37.4	All	All	All
Operating System	Linux	Linux Kernel	2.6.37.5	All	All	All
Operating System	Linux	Linux Kernel	2.6.37	All	All	All
Operating System	Linux	Linux Kernel	2.6.37	rc1	All	All
Operating System	Linux	Linux Kernel	2.6.37	rc2	All	All
Operating System	Linux	Linux Kernel	2.6.37	rc3	All	All

Operating System	Linux	Linux Kernel	2.6.37	rc4	All	All
Operating System	Linux	Linux Kernel	2.6.37	rc5	All	All
Operating System	Linux	Linux Kernel	2.6.37.1	All	All	All
Operating System	Linux	Linux Kernel	2.6.37.2	All	All	All
Operating System	Linux	Linux Kernel	2.6.37.3	All	All	All
Operating System	Linux	Linux Kernel	2.6.37.4	All	All	All
Operating System	Linux	Linux Kernel	2.6.37.5	All	All	All
Operating System	Linux	Linux Kernel	All	All	All	All

cpe:2.3:o:linux:linux_kernel:2.6.37:*:*:*:*:*:*:*:

cpe:2.3:o:linux:linux_kernel:2.6.37:rc1:*:*:*:*:*:*:

cpe:2.3:o:linux:linux_kernel:2.6.37:rc2:*:*:*:*:*:*:

cpe:2.3:o:linux:linux_kernel:2.6.37:rc3:*:*:*:*:*:*:

cpe:2.3:o:linux:linux_kernel:2.6.37:rc4:*:*:*:*:*:*:

cpe:2.3:o:linux:linux_kernel:2.6.37:rc5:*:*:*:*:*:*:

cpe:2.3:o:linux:linux_kernel:2.6.37.1:*:*:*:*:*:*:*:

cpe:2.3:o:linux:linux_kernel:2.6.37.2:*:*:*:*:*:*:*:

cpe:2.3:o:linux:linux_kernel:2.6.37.3:*:*:*:*:*:*:*:

cpe:2.3:o:linux:linux_kernel:2.6.37.4:*:*:*:*:*:*:*:

cpe:2.3:o:linux:linux_kernel:2.6.37.5:*:*:*:*:*:*:*:

cpe:2.3:o:linux:linux_kernel:2.6.37:*:*:*:*:*:*:*:

cpe:2.3:o:linux:linux_kernel:2.6.37:rc1:*:*:*:*:*:*:

cpe:2.3:o:linux:linux_kernel:2.6.37:rc2:*:*:*:*:*:*:

cpe:2.3:o:linux:linux_kernel:2.6.37:rc3:*:*:*:*:*:*:

cpe:2.3:o:linux:linux_kernel:2.6.37:rc4:*:*:*:*:*:*:

cpe:2.3:o:linux:linux_kernel:2.6.37:rc5:*:*:*:*:*:*:

cpe:2.3:o:linux:linux_kernel:2.6.37.1:*:*:*:*:*:*:*:

cpe:2.3:o:linux:linux_kernel:2.6.37.2:*:*:*:*:*:*:*:

cpe:2.3:o:linux:linux_kernel:2.6.37.2:*:*:*:*:*:*:*:

cpe:2.3:o:linux:linux_kernel:2.6.37.3:*:*:*:*:*:*:*:

cpe:2.3:o:linux:linux_kernel:2.6.37.4:*:*:*:*:*:*:*:

cpe:2.3:o:linux:linux_kernel:2.6.37.5:*:*:*:*:*:*:*:

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

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→