CVE-2011-0695

MITRE | NVD | CVE.ORG | JSON API | Print: PDF

Summary

CVE	CVE-2011-0695
State	PUBLIC
Assigner	secalert@redhat.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2011-03-15 17:55:00 UTC
Updated	2020-08-11 20:17:00 UTC
Description	Race condition in the cm_work_handler function in the InfiniBand driver (drivers/infiniband/core/cma.c) in Linux kernel 2.6.x

Risk And Classification

Problem Types: CWE-362

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Canonical	Ubuntu Linux	8.04	All	All	All
Operating System	Canonical	Ubuntu Linux	8.04	All	All	All
Operating System	Linux	Linux Kernel	All	All	All	All
Operating System	Redhat	Enterprise Linux Desktop	5.0	All	All	All
Operating System	Redhat	Enterprise Linux Desktop	5.0	All	All	All
Operating System	Redhat	Enterprise Linux Eus	5.6	All	All	All
Operating System	Redhat	Enterprise Linux Eus	5.6	All	All	All
Operating System	Redhat	Enterprise Linux Server	5.0	All	All	All
Operating System	Redhat	Enterprise Linux Server	5.0	All	All	All
Operating System	Redhat	Enterprise Linux Server Aus	5.6	All	All	All
Operating System	Redhat	Enterprise Linux Server Aus	5.6	All	All	All
Operating System	Redhat	Enterprise Linux Workstation	5.0	All	All	All
Operating System	Redhat	Enterprise Linux Workstation	5.0	All	All	All

References

Reference	Source	Link
access.redhat.com	REDHAT	rhn.r

Linux Kernel InfiniBand Request Handling Denial of Service - Secunia.com	SECUNIA	secu
oss-security - CVE-2011-0695 kernel: panic in ib_cm:cm_work_handler	MLIST	www
USN-1146-1: Linux kernel vulnerabilities | Ubuntu	UBUNTU	www
Linux Kernel Request Handling 'cm.c' Denial of Service Vulnerability	BID	www
IBM X-Force Exchange	XF	exch
[PATCH 1/2] rdma/cm: Fix crash in request handlers — Linux RDMA and InfiniBand development	MLIST	www
[PATCH 2/2] ib/cm: Bump reference count on cm_id before invoking callback — Linux RDMA and InfiniBand development	MLIST	www
CVE Program record	CVE.ORG	www
NVD vulnerability detail	NVD	nvd.

No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.