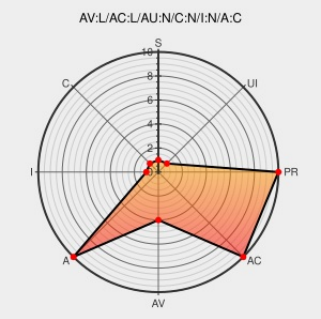
CVE-2011-2491

Published on: 03/01/2013 12:00:00 AM UTC

Last Modified on: 02/13/2023 04:31:00 AM UTC

CVE-2011-2491

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



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

The Network Lock Manager (NLM) protocol implementation in the NFS client functionality in the Linux kernel before 3.0 allows local users to cause a denial of service (system hang) via a LOCK_UN flock system call.

CVE-2011-2491 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
access.redhat.com	Third Party Advisory, web.archive.org, text/html, Inactive Link, Not Archived	REDHAT RHSA-2011:1212
oss-security - Re: CVE request: kernel: NLM: Don't hang forever on NLM unlock requests	Mailing List, Patch, Third Party Advisory, www.openwall.com, text/html	MLIST [oss-security] 20110623 Re: CVE request: kernel: NLM: Don't hang forever on NLM unlock requests
404 Not Found	Broken Link, ftp.osuosl.org, text/plain, Inactive Link, Not Archived	CONFIRM ftp.osuosl.org/pub/linux/kernel/v3.0/ChangeLog-3.0
Bug 709393 – CVE-2011-	Issue Tracking	CONFIRM bugzilla.redhat.com/show_bug.cgi?id=709393

2491 kernel: rpc task leak after flock()ing NFS share	Patch Third Party Advisory bugzilla.redhat.com text/html	
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=0b760113a3a155269a3fba93a409c640031dd68f
NLM: Don't hang forever on NLM unlock requests · torvalds/linux@0b76011 · GitHub	Patch Third Party Advisory github.com text/html	CONFIRM github.com/torvalds/linux/commit/0b760113a3a155269a3fba93a409c640031dd68f

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	All	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 Server	5.0	All	All	All
Operating System	Redhat	Enterprise Linux Server	5.0	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

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

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

cpe:2.3:o:redhat:enterprise_linux_desktop:5.0:*:*:*:*:*:*:*:

cpe:2.3:o:redhat:enterprise_linux_desktop:5.0:*:*:*:*:*:*:*:

cpe:2.3:o:redhat:enterprise_linux_server:5.0:*:*:*:*:*:*:*:

cpe:2.3:o:redhat:enterprise_linux_server:5.0:*:*:*:*:*:*:*:

cpe:2.3:o:redhat:enterprise_linux_workstation:5.0:*:*:*:*:*:*:*:

cpe:2.3:o:redhat:enterprise_linux_workstation:5.0:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→