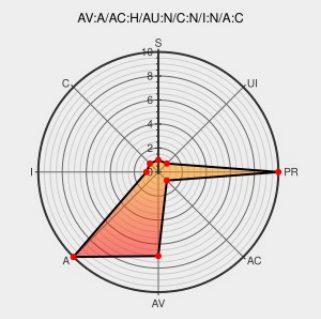
CVE-2011-4131

Published on: 05/17/2012 12:00:00 AM UTC

Last Modified on: 02/13/2023 04:32:00 AM UTC

CVE-2011-4131

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



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

The NFSv4 implementation in the Linux kernel before 3.2.2 does not properly handle bitmap sizes in GETACL replies, which allows remote NFS servers to cause a denial of service (OOPS) by sending an excessive number of bitmap words.

CVE-2011-4131 has been assigned by secalert@redhat.com to track the vulnerability

CVSS2 Score: 4.6 - MEDIUM

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

CVE References

Description	Tags	Link
[security-announce] SUSE-SU-2012:0554-1: important: Security update for	lists.opensuse.org text/html	SUSE SUSE-SU-2012:0554
[SECURITY] Fedora 16 Update: kernel-3.3.7-1.fc16	lists.fedoraproject.org text/html	FEDORA FEDORA-2012-8359
[security-announce] openSUSE-SU-2013:0925-1: important: kernel: security	lists.opensuse.org text/html	SUSE openSUSE-SU-2013:0925
NFSv4: include bitmap in nfsv4 get acl data · torvalds/linux@bf118a3 · GitHub	github.com text/html	CONFIRM github.com/torvalds/linux/commit/bf118a342f10dafe44b14451a1392c3254629a1f

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=bf118a342f10dafe44b14451a1392c3254629a1f
access.redhat.com	web.archive.org text/html Inactive Link Not Archived	REDHAT RHSA-2012:0862
Bug 747106 – CVE-2011-4131 kernel: nfs4_getfacl decoding kernel oops	bugzilla.redhat.com text/html	CONFIRM bugzilla.redhat.com/show_bug.cgi?id=747106
Red Hat Customer Portal	web.archive.org text/html Inactive Link Not Archived	REDHAT RHSA-2012:1541
	www.kernel.org text/plain	CONFIRM www.kernel.org/pub/linux/kernel/v3.x/ChangeLog-3.2.2
oss-security - Re: CVE Request -- kernel: nfs4_getfacl decoding kernel oops	www.openwall.com text/html	MLIST [oss-security] 20111111 Re: CVE Request -- kernel: nfs4_getfacl decoding kernel oops
Security Advisory SA48898 - SUSE update for kernel - Secunia	web.archive.org text/html	SECUNIA 48898

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	3.2	All	All	All
Operating System	Linux	Linux Kernel	3.2	rc2	All	All
Operating System	Linux	Linux Kernel	3.2	rc3	All	All
Operating System	Linux	Linux Kernel	3.2	rc4	All	All
Operating System	Linux	Linux Kernel	3.2	rc5	All	All
Operating System	Linux	Linux Kernel	3.2	rc6	All	All
Operating System	Linux	Linux Kernel	3.2	rc7	All	All
Operating System	Linux	Linux Kernel	3.2.1	All	All	All
Operating	Linux	Linux Kernel	3.2	All	All	All

System						
Operating System	Linux	Linux Kernel	3.2	rc2	All	All
Operating System	Linux	Linux Kernel	3.2	rc3	All	All
Operating System	Linux	Linux Kernel	3.2	rc4	All	All
Operating System	Linux	Linux Kernel	3.2	rc5	All	All
Operating System	Linux	Linux Kernel	3.2	rc6	All	All
Operating System	Linux	Linux Kernel	3.2	rc7	All	All
Operating System	Linux	Linux Kernel	3.2.1	All	All	All

cpe:2.3:o:linux:linux_kernel:3.2:*:*:*:*:*:*:*:

cpe:2.3:o:linux:linux_kernel:3.2:rc2:*:*:*:*:*:*:

cpe:2.3:o:linux:linux_kernel:3.2:rc3:*:*:*:*:*:*:

cpe:2.3:o:linux:linux_kernel:3.2:rc4:*:*:*:*:*:*:

cpe:2.3:o:linux:linux_kernel:3.2:rc5:*:*:*:*:*:*:

cpe:2.3:o:linux:linux_kernel:3.2:rc6:*:*:*:*:*:*:

cpe:2.3:o:linux:linux_kernel:3.2:rc7:*:*:*:*:*:*:

cpe:2.3:o:linux:linux_kernel:3.2.1:*:*:*:*:*:*:*:

cpe:2.3:o:linux:linux_kernel:3.2:*:*:*:*:*:*:*:

cpe:2.3:o:linux:linux_kernel:3.2:rc2:*:*:*:*:*:*:

cpe:2.3:o:linux:linux_kernel:3.2:rc3:*:*:*:*:*:*:

cpe:2.3:o:linux:linux_kernel:3.2:rc4:*:*:*:*:*:*:

cpe:2.3:o:linux:linux_kernel:3.2:rc5:*:*:*:*:*:*:

cpe:2.3:o:linux:linux_kernel:3.2:rc6:*:*:*:*:*:*:

cpe:2.3:o:linux:linux_kernel:3.2:rc7:*:*:*:*:*:*:

cpe:2.3:o:linux:linux_kernel:3.2.1:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→

CVE.report and Source URL Uptime Status status.cve.report