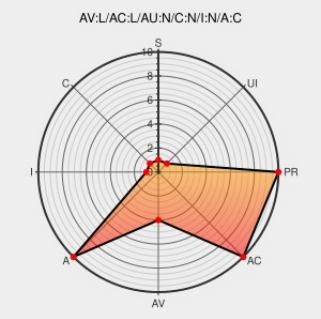
CVE-2011-4324

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

Last Modified on: 02/13/2023 12:21:00 AM UTC

CVE-2011-4324

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



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

The encode_share_access function in fs/nfs/nfs4xdr.c in the Linux kernel before 2.6.29 allows local users to cause a denial of service (BUG and system crash) by using the mknod system call with a pathname on an NFSv4 filesystem.

CVE-2011-4324 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
404 Not Found	ftp.osuosl.org, text/plain, Inactive Link, Not Archived	CONFIRM ftp.osuosl.org/pub/linux/kernel/v2.6/ChangeLog-2.6.29
oss-security - Re: CVE-2011-4324 kernel: nfsv4: mknod(2) DoS	www.openwall.com, text/html	MLIST [oss-security] 20120206 Re: CVE-2011-4324 kernel: nfsv4: mknod(2) DoS
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=dc0b027dfadfcb8a5504f7d8052754bf8d501ab9
755440 – (CVE-2011-4324) CVE-2011-4324 kernel: nfsv4: mknod(2) DoS	bugzilla.redhat.com, text/html	CONFIRM bugzilla.redhat.com/show_bug.cgi?id=755440
NFSv4: Convert the open	Exploit	CONFIRM

and close ops to use fmode · torvalds/linux@dc0b027 · GitHub	Patch github.com text/html	github.com/torvalds/linux/commit/dc0b027dfadfcb8a5504f7d8052754bf8d501ab9

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	2.6.28	All	All	All
Operating System	Linux	Linux Kernel	2.6.28.1	All	All	All
Operating System	Linux	Linux Kernel	2.6.28.2	All	All	All
Operating System	Linux	Linux Kernel	2.6.28.3	All	All	All
Operating System	Linux	Linux Kernel	2.6.28.4	All	All	All
Operating System	Linux	Linux Kernel	2.6.28.5	All	All	All
Operating System	Linux	Linux Kernel	2.6.28.6	All	All	All
Operating System	Linux	Linux Kernel	2.6.28.7	All	All	All
Operating System	Linux	Linux Kernel	2.6.28.8	All	All	All
Operating System	Linux	Linux Kernel	2.6.28.9	All	All	All
Operating System	Linux	Linux Kernel	2.6.28	All	All	All
Operating System	Linux	Linux Kernel	2.6.28.1	All	All	All
Operating System	Linux	Linux Kernel	2.6.28.2	All	All	All
Operating System	Linux	Linux Kernel	2.6.28.3	All	All	All
Operating System	Linux	Linux Kernel	2.6.28.4	All	All	All
Operating System	Linux	Linux Kernel	2.6.28.5	All	All	All
Operating System	Linux	Linux Kernel	2.6.28.6	All	All	All

System						
Operating System	Linux	Linux Kernel	2.6.28.7	All	All	All
Operating System	Linux	Linux Kernel	2.6.28.8	All	All	All
Operating System	Linux	Linux Kernel	2.6.28.9	All	All	All
Operating System	Linux	Linux Kernel	All	All	All	All

- cpe:2.3:o:linux:linux_kernel:2.6.28:*:*:*:*:*:*:*:
- cpe:2.3:o:linux:linux_kernel:2.6.28.1:*:*:*:*:*:*:*:
- cpe:2.3:o:linux:linux_kernel:2.6.28.2:*:*:*:*:*:*:*:
- cpe:2.3:o:linux:linux_kernel:2.6.28.3:*:*:*:*:*:*:*:
- cpe:2.3:o:linux:linux_kernel:2.6.28.4:*:*:*:*:*:*:*:
- cpe:2.3:o:linux:linux_kernel:2.6.28.5:*:*:*:*:*:*:*:
- cpe:2.3:o:linux:linux_kernel:2.6.28.6:*:*:*:*:*:*:*:
- cpe:2.3:o:linux:linux_kernel:2.6.28.7:*:*:*:*:*:*:*:
- cpe:2.3:o:linux:linux_kernel:2.6.28.8:*:*:*:*:*:*:*:
- cpe:2.3:o:linux:linux_kernel:2.6.28.9:*:*:*:*:*:*:*:
- cpe:2.3:o:linux:linux_kernel:2.6.28:*:*:*:*:*:*:*:
- cpe:2.3:o:linux:linux_kernel:2.6.28.1:*:*:*:*:*:*:*:
- cpe:2.3:o:linux:linux_kernel:2.6.28.2:*:*:*:*:*:*:*:
- cpe:2.3:o:linux:linux_kernel:2.6.28.3:*:*:*:*:*:*:*:
- cpe:2.3:o:linux:linux_kernel:2.6.28.4:*:*:*:*:*:*:*:
- cpe:2.3:o:linux:linux_kernel:2.6.28.5:*:*:*:*:*:*:*:
- cpe:2.3:o:linux:linux_kernel:2.6.28.6:*:*:*:*:*:*:*:
- cpe:2.3:o:linux:linux_kernel:2.6.28.7:*:*:*:*:*:*:*:
- cpe:2.3:o:linux:linux_kernel:2.6.28.8:*:*:*:*:*:*:*:
- cpe:2.3:o:linux:linux_kernel:2.6.28.9:*:*:*:*:*:*:*:
- cpe:2.3:o:linux:linux_kernel:*:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→