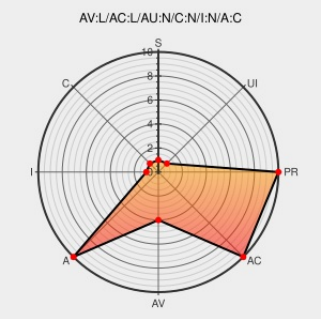
CVE-2011-2695

Published on: 07/28/2011 12:00:00 AM UTC

Last Modified on: 02/13/2023 12:18:00 AM UTC

CVE-2011-2695

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



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

Multiple off-by-one errors in the ext4 subsystem in the Linux kernel before 3.0-rc5 allow local users to cause a denial of service (BUG_ON and system crash) by accessing a sparse file in extent format with a write operation involving a block number corresponding to the largest possible 32-bit unsigned integer.

CVE-2011-2695 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=f17722f917b2f21497deb6edc62fb1683daa08e6
oss-security - CVE Request -- kernel: ext4: kernel panic when writing data to the last block of sparse file	Mailing List, Third Party Advisory, www.openwall.com, text/html	MLIST [oss-security] 20110715 CVE Request -- kernel: ext4: kernel panic when writing data to the last block of sparse file
Linux Kernel GFS2 / ext4 Denial of Service Vulnerabilities - Secunia.com	Third Party Advisory, web.archive.org, text/html	SECUNIA 45193
oss-security - Re: CVE Request -- kernel: ext4: kernel panic when	Mailing List, Third Party Advisory	MLIST [oss-security] 20110715 Re: CVE Request -- kernel: ext4: kernel panic when writing data to the last block of sparse file

writing data to the last block of sparse file	www.openwall.com text/html	
404: File not found	Broken Link www.kernel.org text/html Inactive Link Not Archived	CONFIRM www.kernel.org/pub/linux/kernel/v3.0/testing/ChangeLog-3.0-rc5
Bug 722557 – CVE-2011-2695 kernel: ext4: kernel panic when writing data to the last block of sparse file	Issue Tracking Patch Third Party Advisory bugzilla.redhat.com text/html	CONFIRM bugzilla.redhat.com/show_bug.cgi?id=722557
[PATCH 1/2] ext4: Fix max file size and logical block counting of extent format file (Linux Ext4)	Exploit Patch Third Party Advisory www.spinics.net text/html	MLIST [linux-ext4] 20110603 [PATCH 1/2] ext4: Fix max file size and logical block counting of extent format file

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	3.0	-	All	All
Operating System	Linux	Linux Kernel	3.0	rc1	All	All
Operating System	Linux	Linux Kernel	3.0	rc2	All	All
Operating System	Linux	Linux Kernel	3.0	rc3	All	All
Operating System	Linux	Linux Kernel	3.0	rc4	All	All
Operating System	Linux	Linux Kernel	All	All	All	All
Operating System	Linux	Linux Kernel	3.0	-	All	All
Operating System	Linux	Linux Kernel	3.0	rc1	All	All
Operating System	Linux	Linux Kernel	3.0	rc2	All	All
Operating System	Linux	Linux Kernel	3.0	rc3	All	All

Operating System	Linux	Linux Kernel	3.0	rc4	All	All

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

cpe:2.3:o:linux:linux_kernel:3.0:-:*:*:*:*:*:*:

cpe:2.3:o:linux:linux_kernel:3.0:rc1:*:*:*:*:*:*:

cpe:2.3:o:linux:linux_kernel:3.0:rc2:*:*:*:*:*:*:

cpe:2.3:o:linux:linux_kernel:3.0:rc3:*:*:*:*:*:*:

cpe:2.3:o:linux:linux_kernel:3.0:rc4:*:*:*:*:*:*:

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

cpe:2.3:o:linux:linux_kernel:3.0:-:*:*:*:*:*:*:

cpe:2.3:o:linux:linux_kernel:3.0:rc1:*:*:*:*:*:*:

cpe:2.3:o:linux:linux_kernel:3.0:rc2:*:*:*:*:*:*:

cpe:2.3:o:linux:linux_kernel:3.0:rc3:*:*:*:*:*:*:

cpe:2.3:o:linux:linux_kernel:3.0:rc4:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→