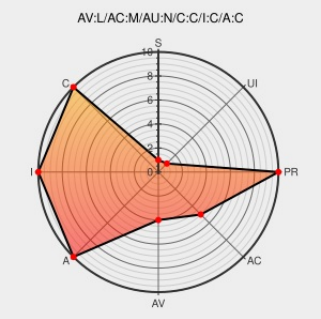
CVE-2011-4077

Published on: 01/27/2012 12:00:00 AM UTC

Last Modified on: 07/27/2023 03:21:00 PM UTC

CVE-2011-4077

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



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

Buffer overflow in the xfs_readlink function in fs/xfs/xfs_vnodeops.c in XFS in the Linux kernel 2.6, when CONFIG_XFS_DEBUG is disabled, allows local users to cause a denial of service (memory corruption and crash) and possibly execute arbitrary code via an XFS image containing a symbolic link with a long pathname.

CVE-2011-4077 has been assigned by secalert@redhat.com to track the vulnerability

CVSS2 Score: 6.9 - MEDIUM

Access Vector	Access Complexity	Authentication
LOCAL	MEDIUM	NONE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
COMPLETE	COMPLETE	COMPLETE

CVE References

Description	Tags	Link
CVE-2011-4077: Linux kernel XFS readlink() Memory Corruption « xorl %eax, %eax	Exploit xorl.wordpress.com text/html	MISC xorl.wordpress.com/2011/12/07/cve-2011-4077-linux-kernel-xfs-readlink-memory-corruption/
Bug 749156 – CVE-2011-4077 kernel: xfs: potential buffer overflow in xfs_readlink()	Patch bugzilla.redhat.com text/html	CONFIRM bugzilla.redhat.com/show_bug.cgi?id=749156
oss-security - CVE Request -- kernel: xfs: potential buffer overflow in xfs_readlink()	Patch www.openwall.com text/html	MLIST [oss-security] 20111026 CVE Request -- kernel: xfs: potential buffer overflow in xfs_readlink()
'[security bulletin] HPSBGN02970 rev.1 - HP Rapid Deployment Pack (RDP) or HP Insight Control Server ' - MARC	marc.info text/html	HP HPSBGN02970

[PATCH] Fix possible memory corruption in xfs_readlink	Patch web.archive.org text/html Inactive Link Not Archived	MLIST [xfs] 20111018 [PATCH] Fix possible memory corruption in xfs_readlink
About Secunia Research | Flexera	secunia.com Depreciated Link text/plain	SECUNIA 48964
oss-security - Re: CVE Request -- kernel: xfs: potential buffer overflow in xfs_readlink()	Patch www.openwall.com text/html	MLIST [oss-security] 20111026 Re: CVE Request -- kernel: xfs: potential buffer overflow in xfs_readlink()

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	2.6.0	All	All	All
Operating System	Linux	Linux Kernel	2.6.0	All	All	All

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

cpe:2.3:o:linux:linux_kernel:2.6.0:*:*:*:*:*:*:*:

cpe:2.3:o:linux:linux_kernel:2.6.0:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→