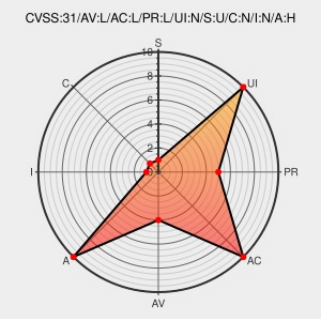
CVE-2011-3353

Published on: 05/24/2012 12:00:00 AM UTC

Last Modified on: 02/13/2023 01:20:00 AM UTC

CVE-2011-3353

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



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

Buffer overflow in the fuse_notify_inval_entry function in fs/fuse/dev.c in the Linux kernel before 3.1 allows local users to cause a denial of service (BUG_ON and system crash) by leveraging the ability to mount a FUSE filesystem.

CVE-2011-3353 has been assigned by secalert@redhat.com to track the vulnerability - currently rated as MEDIUM severity.

CVSS3 Score: 5.5 - MEDIUM

Attack Vector	Attack Complexity	Privileges Required	User Interaction
LOCAL	LOW	LOW	NONE
Scope	**Confidentiality Impact**	**Integrity Impact**	**Availability Impact**
UNCHANGED	NONE	NONE	HIGH

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
fuse: check size of FUSE_NOTIFY_INVAL_ENTRY message · torvalds/linux@c2183d1 · GitHub	Patch, Third Party Advisory, github.com, text/html	CONFIRM github.com/torvalds/linux/commit/c2183d1e9b3f313dd8ba2b1b0197c8d9fb86a

	Mailing List Patch Vendor Advisory www.kernel.org text/plain	CONFIRM www.kernel.org/pub/linux/kernel/v3.x/ChangeLog-3.1
kernel/git/torvalds/linux.git - Linux kernel source tree	Mailing List Patch Vendor Advisory 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=c2183d1e9b3f313dd8ba2b1b0197c8d9fb86a7ae
oss-security - Re: CVE request -- kernel: fuse: check size of FUSE_NOTIFY_INVAL_ENTRY message	Mailing List Patch Third Party Advisory www.openwall.com text/html	MLIST [oss-security] 20110909 Re: CVE request -- kernel: fuse: check size FUSE_NOTIFY_INVAL_ENTRY message
Bug 736761 – CVE-2011-3353 kernel: fuse: check size of FUSE_NOTIFY_INVAL_ENTRY message	Issue Tracking Patch Third Party Advisory bugzilla.redhat.com text/html	CONFIRM bugzilla.redhat.com/show_bug.cgi?id=736761

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

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

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

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→

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