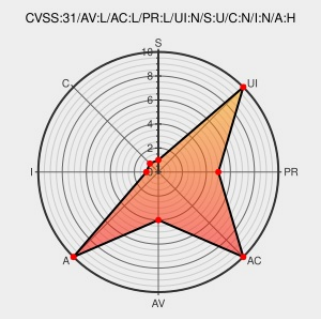
CVE-2011-2479

Published on: 03/01/2013 12:00:00 AM UTC

Last Modified on: 02/13/2023 04:31:00 AM UTC

CVE-2011-2479

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



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

The Linux kernel before 2.6.39 does not properly create transparent huge pages in response to a MAP_PRIVATE mmap system call on /dev/zero, which allows local users to cause a denial of service (system crash) via a crafted application.

CVE-2011-2479 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
mm: thp: fix /dev/zero MAP_PRIVATE and vm_flags cleanups · torvalds/linux@78f11a2 · GitHub	Exploit, Patch, Third Party Advisory, github.com, text/html	CONFIRM github.com/torvalds/linux/commit/78f11a255749d09025f54d4e2df4fbcb031530e2

oss-security - Re: CVE request: kernel: thp: madvise on top of /dev/zero private mapping can lead to panic	Mailing List Third Party Advisory www.openwall.com text/html	MLIST [oss-security] 20110620 Re: CVE request: kernel: thp: madvise on top of /dev/zero private mapping can lead to panic
kernel/git/torvalds/linux.git - Linux kernel source tree	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=78f11a255749d09025f54d4e2df4fbcb031530e2
404 Not Found	Third Party Advisory ftp.osuosl.org text/plain Inactive Link Not Archived	CONFIRM ftp.osuosl.org/pub/linux/kernel/v2.6/ChangeLog-2.6.39
Bug 714761 – CVE-2011-2479 kernel: thp: madvise on top of /dev/zero private mapping can lead to panic	Issue Tracking Third Party Advisory bugzilla.redhat.com text/html	CONFIRM bugzilla.redhat.com/show_bug.cgi?id=714761

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→