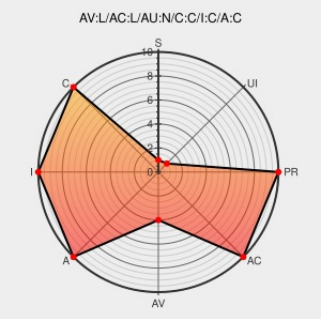
CVE-2011-2184

Published on: 09/06/2011 12:00:00 AM UTC

Last Modified on: 02/13/2023 12:17:00 AM UTC

CVE-2011-2184

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



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

The key_replace_session_keyring function in security/keys/process_keys.c in the Linux kernel before 2.6.39.1 does not initialize a certain structure member, which allows local users to cause a denial of service (NULL pointer dereference and OOPS) or possibly have unspecified other impact via a KEYCTL_SESSION_TO_PARENT argument to the keyctl function, a different vulnerability than CVE-2010-2960.

CVE-2011-2184 has been assigned by secalert@redhat.com to track the vulnerability

CVSS2 Score: 7.2 - HIGH

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

CVE References

Description	Tags	Link
LKML: =?UTF-8?B?Um9iZXJ0IMWad2nEmWNraQ==?=: Re: Fwd: Oops (bad memory deref) in slab_alloc() due to filp_cachep holding incorrect values	Third Party Advisory, lkml.org, text/xml	MLIST [linux-kernel] 20110524 Re: Fwd: Oops (bad memory deref) in slab_alloc() due to filp_cachep holding incorrect values
linux kernel 2.6.39 cred->user_ns in key_replace_session_keyring - SecurityReason.com	Patch, Third Party Advisory, securityreason.com, text/html	SREASON 8371

404: File not found	Broken Link www.kernel.org text/html Inactive Link Not Archived	CONFIRM www.kernel.org/pub/linux/kernel/v2.6/ChangeLog-2.6.39.1
oss-security - Re: CVE request: kernel: set cred->user_ns in key_replace_session_keyring	Mailing List Patch Third Party Advisory www.openwall.com text/html	MLIST [oss-security] 20110606 Re: CVE request: kernel: set cred->user_ns in key_replace_session_keyring
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=f7285b5d631fd6096b11c6af0058ed3a2b30ef4e
oss-security - CVE request: kernel: set cred->user_ns in key_replace_session_keyring	Mailing List Patch Third Party Advisory www.openwall.com text/html	MLIST [oss-security] 20110603 CVE request: kernel: set cred->user_ns in key_replace_session_keyring
No Description Provided	Broken Link alt.swiecki.net Inactive Link Not Archived	MISC alt.swiecki.net/linux_kernel/sys_open-kmem_cache_alloc-2.6.39-rc4.txt
LKML: =?UTF-8?B?Um9iZXJ0IMWad2nEmWNraQ==?=: Oops (bad memory deref) in slab_alloc() due to filp_cachep holding incorrect values	Third Party Advisory lkml.org text/xml	MLIST [linux-kernel] 20110523 Oops (bad memory deref) in slab_alloc() due to filp_cachep holding incorrect values
LKML: Serge Hallyn: Re: [Security] Fwd: Oops (bad memory deref) in slab_alloc() due to filp_cachep holding incorrect values	Patch Third Party Advisory lkml.org text/xml	MLIST [linux-kernel] 20110525 Re: [Security] Fwd: Oops (bad memory deref) in slab_alloc() due to filp_cachep holding incorrect values

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

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→

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