



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

LOCAL

Access
Complexity

LOW

Authentication

NONE

Confidentiality
Impact

COMPLETE

Integrity
Impact

COMPLETE

Availability
Impact

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](#)

[LKML](#) 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](#)

[CX](#) 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

By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to comment@cve.report.

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](#) 2023   |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

CVE.report and Source URL Uptime Status [status.cve.report](#)