



CVE-2010-4258

Published on: 12/30/2010 12:00:00 AM UTC

Last Modified on: 02/13/2023 04:28:00 AM UTC

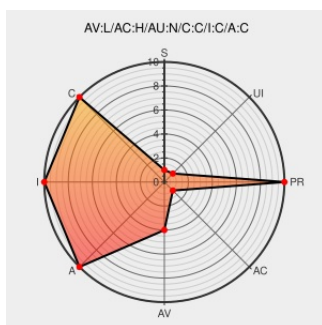
CVE-2010-4258

[Source: Mitre](#)

[Source: NIST](#)

[CVE.ORG](#)

[Print: PDF](#)



Certain versions of [Fedora](#) from [Fedoraproject](#) contain the following vulnerability:

The `do_exit` function in `kernel/exit.c` in the Linux kernel before 2.6.36.2 does not properly handle a `KERNEL_DS` `get_fs` value, which allows local users to bypass intended `access_ok` restrictions, overwrite arbitrary kernel memory locations, and gain privileges by leveraging a (1) BUG, (2) NULL pointer dereference, or (3) page fault, as demonstrated by vectors involving the `clear_child_tid` feature and the `splice` system call.

CVE-2010-4258 has been assigned by secalert@redhat.com to track the vulnerability

CVSS2 Score: **6.2 - MEDIUM**

Access Vector	Access Complexity	Authentication
LOCAL	HIGH	NONE
Confidentiality Impact	Integrity Impact	Availability Impact
COMPLETE	COMPLETE	COMPLETE

CVE References

Description	Tags	Link
SUSE update for kernel - Advisories - Community	Third Party Advisory web.archive.org text/html	SECUNIA 42801
oss-security - kernel: Dangerous interaction between <code>clear_child_tid</code> , <code>set_fs()</code> , and kernel oopses	Mailing List Third Party Advisory openwall.com text/html	MLIST [oss-security] 20101202 kernel: Dangerous interaction between <code>clear_child_tid</code>, <code>set_fs()</code>, and kernel oopses
[security-announce] SUSE Security Announcement: Realtime Linux Kernel (S	Mailing List Third Party Advisory lists.opensuse.org text/html	SUSE SUSE-SA:2011:007

Linux kernel (S	text/html	
oss-security - Re: CVE request: kernel: failure to revert address limit override in OOPS error path	Mailing List Third Party Advisory openwall.com text/html	 MLIST [oss-security] 20101202 Re: CVE request: kernel: failure to revert address limit override in OOPS error path
SUSE update for kernel - Advisories - Community	Third Party Advisory web.archive.org text/html	 SECUNIA 43291
kernel/git/torvalds/linux.git - Linux kernel source tree	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=33dd94ae1ccbf7b7bf0fb6c692bc3d1c4269e6177
oss-security - Re: kernel: Dangerous interaction between clear_child_tid, set_fs(), and kernel oopses	Mailing List Third Party Advisory openwall.com text/html	 MLIST [oss-security] 20101209 Re: kernel: Dangerous interaction between clear_child_tid, set_fs(), and kernel oopses
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH	Third Party Advisory www.vupen.com text/html	 VUPEN ADV-2011-0375
oss-security - CVE request: kernel: failure to revert address limit override in OOPS error path	Mailing List Third Party Advisory openwall.com text/html	 MLIST [oss-security] 20101202 CVE request: kernel: failure to revert address limit override in OOPS error path
[security-announce] SUSE Security Announcement: Linux kernel (SUSE-SA:20	Mailing List Third Party Advisory lists.opensuse.org text/html	 SUSE SUSE-SA:2011:002
[security-announce] SUSE Security Announcement: Linux kernel (SUSE-SA:20	Mailing List Third Party Advisory lists.opensuse.org text/html	 SUSE SUSE-SA:2011:005
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH	Third Party Advisory www.vupen.com text/html	 VUPEN ADV-2011-0012
404: File not found	Broken Link www.kernel.org text/plain Inactive Link Not Archived	 CONFIRM www.kernel.org/pub/linux/kernel/v2.6/ChangeLog-2.6.36.2
SUSE update for kernel - Secunia.com	Third Party Advisory web.archive.org text/html	 SECUNIA 43056
oss-security - Re: kernel: Dangerous interaction between clear_child_tid, set_fs(), and kernel oopses	Mailing List Third Party Advisory openwall.com text/html	 MLIST [oss-security] 20101208 Re: kernel: Dangerous interaction between clear_child_tid, set_fs(), and kernel oopses
oss-security - Re: kernel: Dangerous interaction between clear_child_tid, set_fs(), and kernel oopses	Mailing List Third Party Advisory openwall.com text/html	 MLIST [oss-security] 20101208 Re: kernel: Dangerous interaction between clear_child_tid, set_fs(), and kernel oopses

NEOHAPSIS - Peace of Mind Through Integrity and Insight	Broken Link archives.neohapsis.com text/x-c Inactive Link Not Archived	 FULLDISC 20101207 Linux kernel exploit
Webmail - OVH	Third Party Advisory www.vupen.com text/html	 VUPEN ADV-2011-0213
Bug 659567 – CVE-2010-4258 kernel: failure to revert address limit override in OOPS error path	Issue Tracking Third Party Advisory bugzilla.redhat.com text/html	 CONFIRM bugzilla.redhat.com/show_bug.cgi?id=659567
SUSE update for kernel - Advisories - Community	Third Party Advisory web.archive.org text/html	 SECUNIA 42778
mandriva.com	Third Party Advisory www.mandriva.com text/html	 MANDRIVA MDVSA-2011:029
Sign in - Google Accounts	Third Party Advisory code.google.com text/html	 CONFIRM code.google.com/p/chromium-os/issues/detail?id=10234
LKML: Andrew Morton: Re: [PATCH v2] do_exit(): Make sure we run with get_fs() == USER_DS.	Mailing List Patch Third Party Advisory lkml.org text/xml	 MLIST [linux-kernel] 20101201 Re: [PATCH v2] do_exit(): Make sure we run with get_fs() == USER_DS.
[security-announce] SUSE Security Announcement: Linux kernel (SUSE-SA:20	Mailing List Third Party Advisory lists.opensuse.org text/html	 SUSE SUSE-SA:2011:001
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH	Third Party Advisory www.vupen.com text/html	 VUPEN ADV-2010-3321
Chrome Releases: Chrome OS Beta Channel Update	Third Party Advisory googlechromereleases.blogspot.com text/html	 CONFIRM googlechromereleases.blogspot.com/2011/01/chrome-os-beta-channel-update.html
oss-security - Re: kernel: Dangerous interaction between clear_child_tid, set_fs(), and kernel oopses	Mailing List Third Party Advisory openwall.com text/html	 MLIST [oss-security] 20101202 Re: kernel: Dangerous interaction between clear_child_tid, set_fs(), and kernel oopses
Fedora update for kernel - Advisories - Community	Third Party Advisory web.archive.org text/html	 SECUNIA 42745
[SECURITY] Fedora 13 Update: kernel-2.6.34.7-66.fc13	Third Party Advisory lists.fedoraproject.org text/html	 FEDORA FEDORA-2010-18983
[security-announce] SUSE Security Announcement: Linux kernel (SUSE-SA:20	Mailing List Third Party Advisory lists.opensuse.org text/html	 SUSE SUSE-SA:2011:004
Webmail : Solution de	Third Party Advisory	 VUPEN ADV-2011-0124

Webmail : Solution de messagerie professionnelle - OVHcloud- OVH	Third Party Advisory www.vupen.com text/html	VUPEN ADV-2011-0124
Made of Bugs » CVE-2010-4258: Turning denial-of-service into privilege escalation	Third Party Advisory blog.nelhage.com text/html	MISC blog.nelhage.com/2010/12/cve-2010-4258-from-dos-to-privesc/
SUSE update for kernel - Advisories - Community	Third Party Advisory web.archive.org text/html	SECUNIA 42932
oss-security - Re: kernel: Dangerous interaction between clear_child_tid, set_fs(), and kernel oopses	Mailing List Third Party Advisory openwall.com text/html	MLIST [oss-security] 20101208 Re: kernel: Dangerous interaction between clear_child_tid, set_fs(), and kernel oopses
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH	Third Party Advisory www.vupen.com text/html	VUPEN ADV-2011-0298
oss-security - Re: kernel: Dangerous interaction between clear_child_tid, set_fs(), and kernel oopses	Mailing List Third Party Advisory openwall.com text/x-diff	MLIST [oss-security] 20101209 Re: kernel: Dangerous interaction between clear_child_tid, set_fs(), and kernel oopses
'[PATCH v2] do_exit(): Make sure we run with get_fs() == USER_DS.' - MARC	Patch Third Party Advisory marc.info text/x-diff	MLIST [linux-kernel] 20101201 [PATCH v2] do_exit(): Make sure we run with get_fs() == USER_DS.
[security-announce] SUSE Security Announcement: Linux kernel (SUSE-SA:20	Mailing List Third Party Advisory lists.opensuse.org text/html	SUSE SUSE-SA:2011:008

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

Exploit/POC from Github

Exploit based on a faulty clone(2) implementation in Linux < 2.6.36.2 that allows overwrite of arbitrary kernel word ...

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Fedoraproject	Fedora	13	All	All	All
Operating	Fedoraproject	Fedora	13	All	All	All

Operating System	Fedora Project	Fedora	13	All	All	All
Operating System	Linux	Linux Kernel	All	All	All	All
Operating System	Linux	Linux Kernel	All	All	All	All
Operating System	Opensuse	Opensuse	11.2	All	All	All
Operating System	Opensuse	Opensuse	11.3	All	All	All
Operating System	Opensuse	Opensuse	11.2	All	All	All
Operating System	Opensuse	Opensuse	11.3	All	All	All
Operating System	Suse	Linux Enterprise Desktop	10	sp3	All	All
Operating System	Suse	Linux Enterprise Desktop	11	sp1	All	All
Operating System	Suse	Linux Enterprise Desktop	10	sp3	All	All
Operating System	Suse	Linux Enterprise Desktop	11	sp1	All	All
Operating System	Suse	Linux Enterprise Real Time Extension	11	sp1	All	All
Operating System	Suse	Linux Enterprise Real Time Extension	11	sp1	All	All
Operating System	Suse	Linux Enterprise Server	10	sp3	All	All
Operating System	Suse	Linux Enterprise Server	11	sp1	All	All
Operating System	Suse	Linux Enterprise Server	9	All	All	All
Operating System	Suse	Linux Enterprise Server	10	sp3	All	All
Operating System	Suse	Linux Enterprise Server	11	sp1	All	All
Operating System	Suse	Linux Enterprise Server	9	All	All	All
Operating System	Suse	Linux Enterprise Software Development Kit	10	sp3	All	All
Operating System	Suse	Linux Enterprise Software Development Kit	10	sp3	All	All
cpe:2.3:o:fedoraproject:fedora:13:*****:						
cpe:2.3:o:fedoraproject:fedora:13:*****:						
cpe:2.3:o:linux:linux_kernel:*****:						

cpe:2.3:o:linux:linux_kernel:*:*:*:*:*:*:
cpe:2.3:o:opensuse:opensuse:11.2:*:*:*:*:*:
cpe:2.3:o:opensuse:opensuse:11.3:*:*:*:*:*:
cpe:2.3:o:opensuse:opensuse:11.2:*:*:*:*:*:
cpe:2.3:o:opensuse:opensuse:11.3:*:*:*:*:*:
cpe:2.3:o:suse:linux_enterprise_desktop:10:sp3:*:*:*:*:*:
cpe:2.3:o:suse:linux_enterprise_desktop:11:sp1:*:*:*:*:*:
cpe:2.3:o:suse:linux_enterprise_desktop:10:sp3:*:*:*:*:*:
cpe:2.3:o:suse:linux_enterprise_desktop:11:sp1:*:*:*:*:*:
cpe:2.3:o:suse:linux_enterprise_real_time_extension:11:sp1:*:*:*:*:*:
cpe:2.3:o:suse:linux_enterprise_real_time_extension:11:sp1:*:*:*:*:*:
cpe:2.3:o:suse:linux_enterprise_server:10:sp3:*:*:*:*:*:
cpe:2.3:o:suse:linux_enterprise_server:11:sp1:*:*:*:*:*:
cpe:2.3:o:suse:linux_enterprise_server:9:*:*:*:*:*:
cpe:2.3:o:suse:linux_enterprise_server:10:sp3:*:*:*:*:*:
cpe:2.3:o:suse:linux_enterprise_server:11:sp1:*:*:*:*:*:
cpe:2.3:o:suse:linux_enterprise_server:9:*:*:*:*:*:
cpe:2.3:o:suse:linux_enterprise_software_development_kit:10:sp3:*:*:*:*:*:
cpe:2.3:o:suse:linux_enterprise_software_development_kit:10:sp3:*:*:*:*:*:

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