

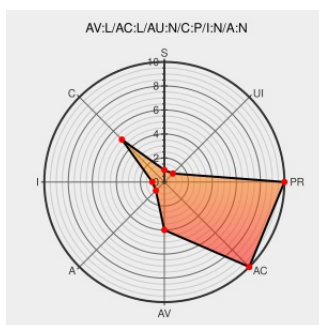


CVE-2010-1636

Published on: 06/07/2010 12:00:00 AM UTC

Last Modified on: 02/13/2023 04:18:00 AM UTC

CVE-2010-1636

[Source: Mitre](#)[Source: NIST](#)[CVE.ORG](#)[Print: PDF](#)

Certain versions of [Linux Kernel](#) from [Linux](#) contain the following vulnerability:

The `btrfs_ioctl_clone` function in `fs/btrfs/ioctl.c` in the `btrfs` functionality in the Linux kernel 2.6.29 through 2.6.32, and possibly other versions, does not ensure that a cloned file descriptor has been opened for reading, which allows local users to read sensitive information from a write-only file descriptor.

CVE-2010-1636 has been assigned by [secalert@redhat.com](#) to track the vulnerability

CVSS2 Score: **2.1 - LOW**

Access
Vector

LOCAL

Access
Complexity

LOW

Authentication

NONE

Confidentiality
Impact

PARTIAL

Integrity
Impact

NONE

Availability
Impact

NONE

CVE References

Description

Tags

Link

kernel/git/torvalds/linux.git -
Linux kernel source tree

[Patch](#)
[web.archive.org](#)
[text/html](#)
[Inactive Link](#) [Not Archived](#)

[MISC git.kernel.org/?p=linux/kernel/git/torvalds/linux-2.6.git%3Ba=commitdiff%3Bh=5dc6416414fb3ec6e2825fd4d20c8bf1d7fe0395](#)

Bug #579585 "btrfs security
issues (information disclosure,
insu..." : Bugs : "linux"
package : Ubuntu

[Exploit](#)
[Patch](#)
[bugs.launchpad.net](#)
[text/html](#)

[MISC bugs.launchpad.net/ubuntu/+source/linux/+bug/579585](#)

oss-security - kernel: btrfs:
check for read permission on
src file in the clone ioctl

[Patch](#)
[www.openwall.com](#)
[text/html](#)

[MLIST \[oss-security\] 20100518 kernel: btrfs: check for read permission on src file in the clone ioctl](#)

593226 – (CVE-2010-1636)

[Exploit](#)

[CONFIRM bugzilla.redhat.com/show_bug.cgi?id=593226](#)

CVE-2010-1636 kernel: btrfs:
check for read permission on
src file in the clone ioctl

bugzilla.redhat.com
[text/html](#)

oss-security - Re: kernel: btrfs:
check for read permission on
src file in the clone ioctl

www.openwall.com
[text/html](#)

 [MLIST \[oss-security\] 20100525 Re: kernel: btrfs: check for read permission on src file in the clone ioctl](#)

oss-security - Re: kernel: btrfs:
check for read permission on
src file in the clone ioctl

www.openwall.com
[text/html](#)

 [MLIST \[oss-security\] 20100518 Re: kernel: btrfs: check for read permission on src file in the clone ioctl](#)

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	2.6.29	All	All	All
Operating System	Linux	Linux Kernel	2.6.29.1	All	All	All
Operating System	Linux	Linux Kernel	2.6.29.2	All	All	All
Operating System	Linux	Linux Kernel	2.6.29.3	All	All	All
Operating System	Linux	Linux Kernel	2.6.29.4	All	All	All
Operating System	Linux	Linux Kernel	2.6.29.5	All	All	All
Operating System	Linux	Linux Kernel	2.6.29.6	All	All	All
Operating System	Linux	Linux Kernel	2.6.30	All	All	All
Operating System	Linux	Linux Kernel	2.6.30.1	All	All	All
Operating System	Linux	Linux Kernel	2.6.30.10	All	All	All
Operating System	Linux	Linux Kernel	2.6.30.2	All	All	All
Operating System	Linux	Linux Kernel	2.6.30.3	All	All	All
Operating System	Linux	Linux Kernel	2.6.30.4	All	All	All
Operating System	Linux	Linux Kernel	2.6.30.5	All	All	All

Operating System	Linux	Linux Kernel	2.6.30.6	All	All	All
Operating System	Linux	Linux Kernel	2.6.30.7	All	All	All
Operating System	Linux	Linux Kernel	2.6.30.8	All	All	All
Operating System	Linux	Linux Kernel	2.6.30.9	All	All	All
Operating System	Linux	Linux Kernel	2.6.31	All	All	All
Operating System	Linux	Linux Kernel	2.6.31.1	All	All	All
Operating System	Linux	Linux Kernel	2.6.31.10	All	All	All
Operating System	Linux	Linux Kernel	2.6.31.11	All	All	All
Operating System	Linux	Linux Kernel	2.6.31.12	All	All	All
Operating System	Linux	Linux Kernel	2.6.31.13	All	All	All
Operating System	Linux	Linux Kernel	2.6.31.2	All	All	All
Operating System	Linux	Linux Kernel	2.6.31.3	All	All	All
Operating System	Linux	Linux Kernel	2.6.31.4	All	All	All
Operating System	Linux	Linux Kernel	2.6.31.5	All	All	All
Operating System	Linux	Linux Kernel	2.6.31.6	All	All	All
Operating System	Linux	Linux Kernel	2.6.31.7	All	All	All
Operating System	Linux	Linux Kernel	2.6.31.8	All	All	All
Operating System	Linux	Linux Kernel	2.6.31.9	All	All	All
Operating System	Linux	Linux Kernel	2.6.32	All	All	All
Operating System	Linux	Linux Kernel	2.6.29	All	All	All
Operating System	Linux	Linux Kernel	2.6.29.1	All	All	All
Operating System	Linux	Linux Kernel	2.6.29.2	All	All	All
Operating System	Linux	Linux Kernel	2.6.29.3	All	All	All

Operating System	Linux	Linux Kernel	2.6.29.4	All	All	All
Operating System	Linux	Linux Kernel	2.6.29.5	All	All	All
Operating System	Linux	Linux Kernel	2.6.29.6	All	All	All
Operating System	Linux	Linux Kernel	2.6.30	All	All	All
Operating System	Linux	Linux Kernel	2.6.30.1	All	All	All
Operating System	Linux	Linux Kernel	2.6.30.10	All	All	All
Operating System	Linux	Linux Kernel	2.6.30.2	All	All	All
Operating System	Linux	Linux Kernel	2.6.30.3	All	All	All
Operating System	Linux	Linux Kernel	2.6.30.4	All	All	All
Operating System	Linux	Linux Kernel	2.6.30.5	All	All	All
Operating System	Linux	Linux Kernel	2.6.30.6	All	All	All
Operating System	Linux	Linux Kernel	2.6.30.7	All	All	All
Operating System	Linux	Linux Kernel	2.6.30.8	All	All	All
Operating System	Linux	Linux Kernel	2.6.30.9	All	All	All
Operating System	Linux	Linux Kernel	2.6.31	All	All	All
Operating System	Linux	Linux Kernel	2.6.31.1	All	All	All
Operating System	Linux	Linux Kernel	2.6.31.10	All	All	All
Operating System	Linux	Linux Kernel	2.6.31.11	All	All	All
Operating System	Linux	Linux Kernel	2.6.31.12	All	All	All
Operating System	Linux	Linux Kernel	2.6.31.13	All	All	All
Operating System	Linux	Linux Kernel	2.6.31.2	All	All	All
Operating System	Linux	Linux Kernel	2.6.31.3	All	All	All
Operating System	Linux	Linux Kernel	2.6.31.4	All	All	All

Operating System	Linux	Linux Kernel	2.6.31.5	All	All	All
Operating System	Linux	Linux Kernel	2.6.31.6	All	All	All
Operating System	Linux	Linux Kernel	2.6.31.7	All	All	All
Operating System	Linux	Linux Kernel	2.6.31.8	All	All	All
Operating System	Linux	Linux Kernel	2.6.31.9	All	All	All
Operating System	Linux	Linux Kernel	2.6.32	All	All	All
cpe:2.3:o:linux:linux_kernel:2.6.29:*:*:*:*:*:						
cpe:2.3:o:linux:linux_kernel:2.6.29.1:*:*:*:*:*:						
cpe:2.3:o:linux:linux_kernel:2.6.29.2:*:*:*:*:*:						
cpe:2.3:o:linux:linux_kernel:2.6.29.3:*:*:*:*:*:						
cpe:2.3:o:linux:linux_kernel:2.6.29.4:*:*:*:*:*:						
cpe:2.3:o:linux:linux_kernel:2.6.29.5:*:*:*:*:*:						
cpe:2.3:o:linux:linux_kernel:2.6.29.6:*:*:*:*:*:						
cpe:2.3:o:linux:linux_kernel:2.6.30:*:*:*:*:*:						
cpe:2.3:o:linux:linux_kernel:2.6.30.1:*:*:*:*:*:						
cpe:2.3:o:linux:linux_kernel:2.6.30.10:*:*:*:*:*:						
cpe:2.3:o:linux:linux_kernel:2.6.30.2:*:*:*:*:*:						
cpe:2.3:o:linux:linux_kernel:2.6.30.3:*:*:*:*:*:						
cpe:2.3:o:linux:linux_kernel:2.6.30.4:*:*:*:*:*:						
cpe:2.3:o:linux:linux_kernel:2.6.30.5:*:*:*:*:*:						
cpe:2.3:o:linux:linux_kernel:2.6.30.6:*:*:*:*:*:						
cpe:2.3:o:linux:linux_kernel:2.6.30.7:*:*:*:*:*:						
cpe:2.3:o:linux:linux_kernel:2.6.30.8:*:*:*:*:*:						
cpe:2.3:o:linux:linux_kernel:2.6.30.9:*:*:*:*:*:						
cpe:2.3:o:linux:linux_kernel:2.6.31:*:*:*:*:*:						
cpe:2.3:o:linux:linux_kernel:2.6.31.1:*:*:*:*:*:						
cpe:2.3:o:linux:linux_kernel:2.6.31.10:*:*:*:*:*:						

cpe:2.3:o:linux:linux_kernel:2.6.31.11:****:*:*:
cpe:2.3:o:linux:linux_kernel:2.6.31.12:****:*:*:
cpe:2.3:o:linux:linux_kernel:2.6.31.13:****:*:*:
cpe:2.3:o:linux:linux_kernel:2.6.31.2:****:*:*:
cpe:2.3:o:linux:linux_kernel:2.6.31.3:****:*:*:
cpe:2.3:o:linux:linux_kernel:2.6.31.4:****:*:*:
cpe:2.3:o:linux:linux_kernel:2.6.31.5:****:*:*:
cpe:2.3:o:linux:linux_kernel:2.6.31.6:****:*:*:
cpe:2.3:o:linux:linux_kernel:2.6.31.7:****:*:*:
cpe:2.3:o:linux:linux_kernel:2.6.31.8:****:*:*:
cpe:2.3:o:linux:linux_kernel:2.6.31.9:****:*:*:
cpe:2.3:o:linux:linux_kernel:2.6.32:****:*:*:
cpe:2.3:o:linux:linux_kernel:2.6.29:****:*:*:
cpe:2.3:o:linux:linux_kernel:2.6.29.1:****:*:*:
cpe:2.3:o:linux:linux_kernel:2.6.29.2:****:*:*:
cpe:2.3:o:linux:linux_kernel:2.6.29.3:****:*:*:
cpe:2.3:o:linux:linux_kernel:2.6.29.4:****:*:*:
cpe:2.3:o:linux:linux_kernel:2.6.29.5:****:*:*:
cpe:2.3:o:linux:linux_kernel:2.6.29.6:****:*:*:
cpe:2.3:o:linux:linux_kernel:2.6.30:****:*:*:
cpe:2.3:o:linux:linux_kernel:2.6.30.1:****:*:*:
cpe:2.3:o:linux:linux_kernel:2.6.30.10:****:*:*:
cpe:2.3:o:linux:linux_kernel:2.6.30.2:****:*:*:
cpe:2.3:o:linux:linux_kernel:2.6.30.3:****:*:*:
cpe:2.3:o:linux:linux_kernel:2.6.30.4:****:*:*:
cpe:2.3:o:linux:linux_kernel:2.6.30.5:****:*:*:
cpe:2.3:o:linux:linux_kernel:2.6.30.6:****:*:*:
cpe:2.3:o:linux:linux_kernel:2.6.30.7:****:*:*:

cpe:2.3:o:linux:linux_kernel:2.6.30.8:*****:
cpe:2.3:o:linux:linux_kernel:2.6.30.9:*****:
cpe:2.3:o:linux:linux_kernel:2.6.31:*****:
cpe:2.3:o:linux:linux_kernel:2.6.31.1:*****:
cpe:2.3:o:linux:linux_kernel:2.6.31.10:*****:
cpe:2.3:o:linux:linux_kernel:2.6.31.11:*****:
cpe:2.3:o:linux:linux_kernel:2.6.31.12:*****:
cpe:2.3:o:linux:linux_kernel:2.6.31.13:*****:
cpe:2.3:o:linux:linux_kernel:2.6.31.2:*****:
cpe:2.3:o:linux:linux_kernel:2.6.31.3:*****:
cpe:2.3:o:linux:linux_kernel:2.6.31.4:*****:
cpe:2.3:o:linux:linux_kernel:2.6.31.5:*****:
cpe:2.3:o:linux:linux_kernel:2.6.31.6:*****:
cpe:2.3:o:linux:linux_kernel:2.6.31.7:*****:
cpe:2.3:o:linux:linux_kernel:2.6.31.8:*****:
cpe:2.3:o:linux:linux_kernel:2.6.31.9:*****:
cpe:2.3:o:linux:linux_kernel:2.6.32:*****:

No vendor comments have been submitted for this CVE

[← Previous ID](#)

[Next ID→](#)