

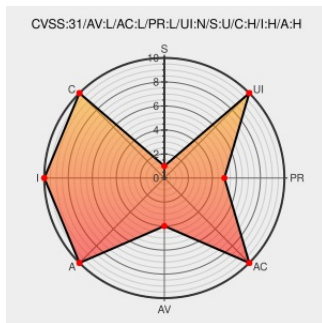


CVE-2011-1771

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

Last Modified on: 02/13/2023 04:30:00 AM UTC

CVE-2011-1771

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

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

The cifs_close function in fs/cifs/file.c in the Linux kernel before 2.6.39 allows local users to cause a denial of service (NULL pointer dereference and BUG) or possibly have unspecified other impact by setting the O_DIRECT flag during an attempt to open a file on a CIFS filesystem.

CVE-2011-1771 has been assigned by secalert@redhat.com to track the vulnerability - currently rated as **HIGH** severity.

CVSS3 Score: **7.8 - HIGH**

Attack Vector	Attack Complexity	Privileges Required	User Interaction
LOCAL	LOW	LOW	NONE
Scope	Confidentiality Impact	Integrity Impact	Availability Impact
UNCHANGED	HIGH	HIGH	HIGH

CVSS2 Score: **4.4 - MEDIUM**

Access Vector	Access Complexity	Authentication
LOCAL	MEDIUM	NONE
Confidentiality Impact	Integrity Impact	Availability Impact
PARTIAL	PARTIAL	PARTIAL

CVE References

Description	Tags	Link
703016 – (CVE-2011-1771) CVE-2011-1771 kernel: cifs oops when creating file with O_DIRECT set	Exploit Issue Tracking Patch Third Party Advisory	CONFIRM bugzilla.redhat.com/show_bug.cgi?id=703016

O_DIRECT set	Third Party Advisory bugzilla.redhat.com text/html	
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=7797069305d13252fd66cf722aa8f2cbeb3c95cd
404: File not found	Release Notes Vendor Advisory www.kernel.org text/html Inactive Link Not Archived	CONFIRM www.kernel.org/pub/linux/kernel/v2.6/ChangeLog-2.6.39
'Re: Repeatable crash in 2.6.38 related to O_DIRECT' - MARC	Third Party Advisory marc.info text/html	MLIST [linux-cifs] 20110405 Re: Repeatable crash in 2.6.38 related to O_DIRECT
linux kernel 2.6.38 related to O_DIRECT crash - SecurityReason.com	Third Party Advisory securityreason.com text/html	SREASON 8367
'Repeatable crash in 2.6.38 related to O_DIRECT' - MARC	Exploit Third Party Advisory marc.info text/html	MLIST [linux-cifs] 20110405 Repeatable crash in 2.6.38 related to O_DIRECT
oss-security - CVE-2011-1771 kernel: cifs oops when creating file with O_DIRECT set	Exploit Mailing List Patch Third Party Advisory www.openwall.com text/html	MLIST [oss-security] 20110509 CVE-2011-1771 kernel: cifs oops when creating file with O_DIRECT set

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

© [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](#)