

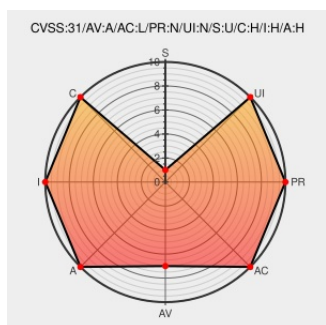


CVE-2011-3191

Published on: 05/24/2012 12:00:00 AM UTC

Last Modified on: 02/13/2023 04:32:00 AM UTC

CVE-2011-3191

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

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

Integer signedness error in the CIFSFindNext function in fs/cifs/cifssmb.c in the Linux kernel before 3.1 allows remote CIFS servers to cause a denial of service (memory corruption) or possibly have unspecified other impact via a large length value in a response to a read request for a directory.

CVE-2011-3191 has been assigned by secalert@redhat.com to track the vulnerability - currently rated as **HIGH** severity.

CVSS3 Score: **8.8 - HIGH**

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

CVSS2 Score: **8.3 - HIGH**

Access Vector	Access Complexity	Authentication
ADJACENT_NETWORK	LOW	NONE
Confidentiality Impact	Integrity Impact	Availability Impact
COMPLETE	COMPLETE	COMPLETE

CVE References

Description	Tags	Link
	Mailing List Patch Vendor Advisory	CONFIRM www.kernel.org/pub/linux/kernel/v3.x/ChangeLog-3.1

[www.kernel.org](#)
[text/plain](#)

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=9438fabb73eb48055b58b89fc51e0bc4db22fabd](#)

Patch
Third Party Advisory
github.com
[text/html](#)

cifs: fix possible memory corruption in CIFSFindNext · torvalds/linux@9438fab · GitHub

CONFIRM [github.com/torvalds/linux/commit/9438fabb73eb48055b58b89fc51e0bc4db22fabd](#)

Issue Tracking
Patch
Third Party Advisory
[bugzilla.redhat.com](#)
[text/html](#)

Bug 732869 – CVE-2011-3191 kernel: cifs: signedness issue in CIFSFindNext()

CONFIRM [bugzilla.redhat.com/show_bug.cgi?id=732869](#)

Mailing List
Patch
Third Party Advisory
[www.openwall.com](#)
[text/html](#)

oss-security - Re: CVE request: kernel: cifs: signedness issue in CIFSFindNext()

MLIST [oss-security] 20110824 Re: CVE request: kernel: cifs: signedness issue in CIFSFindNext()

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
Operating System	Redhat	Enterprise Linux	4.0	All	All	All
Operating System	Redhat	Enterprise Linux	4.0	All	All	All
cpe:2.3:o:linux:linux_kernel:*****:						
cpe:2.3:o:linux:linux_kernel:*****:						
cpe:2.3:o:redhat:enterprise_linux:4.0:*****:						
cpe:2.3:o:redhat:enterprise_linux:4.0:*****:						

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](#)