



CVE-2011-2496

Published on: 06/13/2012 12:00:00 AM UTC

Last Modified on: 02/13/2023 01:19:00 AM UTC

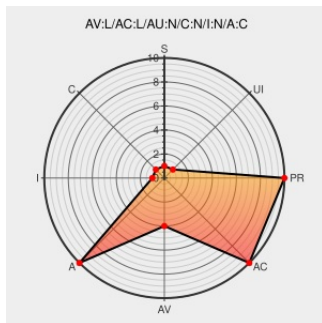
CVE-2011-2496

Source: Mitre

Source: NIST

CVE.ORG

Print: PDF



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

Integer overflow in the vma_to_resize function in mm/mremap.c in the Linux kernel before 2.6.39 allows local users to cause a denial of service (BUG_ON and system crash) via a crafted mremap system call that expands a memory mapping.

CVE-2011-2496 has been assigned by secalert@redhat.com to track the vulnerability

CVSS2 Score: **4.9 - MEDIUM**

Access
Vector

Access
Complexity

Authentication

LOCAL

LOW

NONE

Confidentiality
Impact

Integrity
Impact

Availability
Impact

NONE

NONE

COMPLETE

CVE References

Description

Tags

Link

Bug 716538 – CVE-2011-2496 kernel: mm: avoid wrapping vm_pgoff in mremap() and stack expansions

bugzilla.redhat.com
text/html

CONFIRM bugzilla.redhat.com/show_bug.cgi?id=716538

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=commit%3Bh=982134ba62618c2d69fbbbd166d0a11ee3b7e3d8

mm: avoid wrapping vm_pgoff in mremap() · torvalds/linux@982134b · GitHub

Exploit
Patch
github.com
text/html

CONFIRM github.com/torvalds/linux/commit/982134ba62618c2d69fbbbd166d0a11ee3b7e3d8

404 Not Found

ftp.osuosl.org

CONFIRM ftp.osuosl.org/pub/linux/kernel/v2.6/Channel-aa-2.6.39

oss-security - Re: CVE request: kernel: mm: avoid wrapping vm_pgoff in mremap() and stack expansions

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

 [MLIST \[oss-security\] 20110627 Re: CVE request: kernel: mm: avoid wrapping vm_pgoff in mremap\(\) and stack expansions](#)

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	2.6.38	All	All	All
Operating System	Linux	Linux Kernel	2.6.38	rc1	All	All
Operating System	Linux	Linux Kernel	2.6.38	rc2	All	All
Operating System	Linux	Linux Kernel	2.6.38	rc3	All	All
Operating System	Linux	Linux Kernel	2.6.38	rc4	All	All
Operating System	Linux	Linux Kernel	2.6.38	rc5	All	All
Operating System	Linux	Linux Kernel	2.6.38	rc6	All	All
Operating System	Linux	Linux Kernel	2.6.38	rc7	All	All
Operating System	Linux	Linux Kernel	2.6.38	rc8	All	All
Operating System	Linux	Linux Kernel	2.6.38.1	All	All	All
Operating System	Linux	Linux Kernel	2.6.38.2	All	All	All
Operating System	Linux	Linux Kernel	2.6.38.3	All	All	All
Operating System	Linux	Linux Kernel	2.6.38.4	All	All	All
Operating System	Linux	Linux Kernel	2.6.38.5	All	All	All
Operating System	Linux	Linux Kernel	2.6.38.6	All	All	All

Operating System	Linux	Linux Kernel	2.6.38.7	All	All	All
Operating System	Linux	Linux Kernel	2.6.38	All	All	All
Operating System	Linux	Linux Kernel	2.6.38	rc1	All	All
Operating System	Linux	Linux Kernel	2.6.38	rc2	All	All
Operating System	Linux	Linux Kernel	2.6.38	rc3	All	All
Operating System	Linux	Linux Kernel	2.6.38	rc4	All	All
Operating System	Linux	Linux Kernel	2.6.38	rc5	All	All
Operating System	Linux	Linux Kernel	2.6.38	rc6	All	All
Operating System	Linux	Linux Kernel	2.6.38	rc7	All	All
Operating System	Linux	Linux Kernel	2.6.38	rc8	All	All
Operating System	Linux	Linux Kernel	2.6.38.1	All	All	All
Operating System	Linux	Linux Kernel	2.6.38.2	All	All	All
Operating System	Linux	Linux Kernel	2.6.38.3	All	All	All
Operating System	Linux	Linux Kernel	2.6.38.4	All	All	All
Operating System	Linux	Linux Kernel	2.6.38.5	All	All	All
Operating System	Linux	Linux Kernel	2.6.38.6	All	All	All
Operating System	Linux	Linux Kernel	2.6.38.7	All	All	All
Operating System	Linux	Linux Kernel	All	All	All	All
cpe:2.3:o:linux:linux_kernel:2.6.38:*:*:*:*:*:						
cpe:2.3:o:linux:linux_kernel:2.6.38:rc1:*:*:*:*:*:						
cpe:2.3:o:linux:linux_kernel:2.6.38:rc2:*:*:*:*:*:						
cpe:2.3:o:linux:linux_kernel:2.6.38:rc3:*:*:*:*:*:						
cpe:2.3:o:linux:linux_kernel:2.6.38:rc4:*:*:*:*:*:						
cpe:2.3:o:linux:linux_kernel:2.6.38:rc5:*:*:*:*:*:						

cpe:2.3:o:linux:linux_kernel:2.6.38:rc6:*****:
cpe:2.3:o:linux:linux_kernel:2.6.38:rc7:*****:
cpe:2.3:o:linux:linux_kernel:2.6.38:rc8:*****:
cpe:2.3:o:linux:linux_kernel:2.6.38.1:*****:
cpe:2.3:o:linux:linux_kernel:2.6.38.2:*****:
cpe:2.3:o:linux:linux_kernel:2.6.38.3:*****:
cpe:2.3:o:linux:linux_kernel:2.6.38.4:*****:
cpe:2.3:o:linux:linux_kernel:2.6.38.5:*****:
cpe:2.3:o:linux:linux_kernel:2.6.38.6:*****:
cpe:2.3:o:linux:linux_kernel:2.6.38.7:*****:
cpe:2.3:o:linux:linux_kernel:2.6.38:*****:
cpe:2.3:o:linux:linux_kernel:2.6.38:rc1:*****:
cpe:2.3:o:linux:linux_kernel:2.6.38:rc2:*****:
cpe:2.3:o:linux:linux_kernel:2.6.38:rc3:*****:
cpe:2.3:o:linux:linux_kernel:2.6.38:rc4:*****:
cpe:2.3:o:linux:linux_kernel:2.6.38:rc5:*****:
cpe:2.3:o:linux:linux_kernel:2.6.38:rc6:*****:
cpe:2.3:o:linux:linux_kernel:2.6.38:rc7:*****:
cpe:2.3:o:linux:linux_kernel:2.6.38:rc8:*****:
cpe:2.3:o:linux:linux_kernel:2.6.38.1:*****:
cpe:2.3:o:linux:linux_kernel:2.6.38.2:*****:
cpe:2.3:o:linux:linux_kernel:2.6.38.3:*****:
cpe:2.3:o:linux:linux_kernel:2.6.38.4:*****:
cpe:2.3:o:linux:linux_kernel:2.6.38.5:*****:
cpe:2.3:o:linux:linux_kernel:2.6.38.6:*****:
cpe:2.3:o:linux:linux_kernel:2.6.38.7:*****:
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](#)