



CVE-2011-1759

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

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

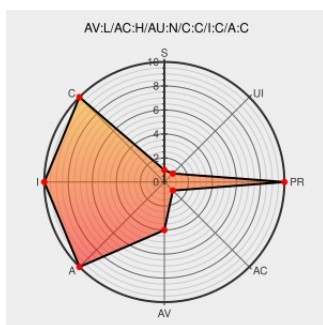
CVE-2011-1759

Source: Mitre

Source: NIST

CVE.ORG

Print: PDF



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

Integer overflow in the sys_oabi_semtimedop function in arch/arm/kernel/sys_oabi_compat.c in the Linux kernel before 2.6.39 on the ARM platform, when CONFIG_OABI_COMPAT is enabled, allows local users to gain privileges or cause a denial of service (heap memory corruption) by providing a crafted argument and leveraging a

race condition.

CVE-2011-1759 has been assigned by secalert@redhat.com to track the vulnerability

CVSS2 Score: **6.2 - MEDIUM**

Access
Vector

LOCAL

Access
Complexity

HIGH

Authentication

NONE

Confidentiality
Impact

COMPLETE

Integrity
Impact

COMPLETE

Availability
Impact

COMPLETE

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=commit%3Bh=0f22072ab50cac7983f9660d33974b45184da4f9](#)

404 Not Found

[ftp.osuosl.org](#)

[text/plain](#)

[Inactive Link](#)

[Not Archived](#)

[CONFIRM ftp.osuosl.org/pub/linux/kernel/v2.6/ChangeLog-2.6.39](#)

oss-security - Re: CVE
request: kernel (ARM):
heap corruption in OABI
semtimedop

[www.openwall.com](#)

[text/html](#)

[MLIST \[oss-security\] 20110502 Re: CVE request: kernel \(ARM\): heap corruption in OABI semtimedop](#)

ARM: 6891/1: prevent heap
corruption in OABI
sentimedop ·
torvalds/linux@0f22072 ·
GitHub

Exploit
Patch
github.com
text/html



CONFIRM

github.com/torvalds/linux/commit/0f22072ab50cac7983f9660d33974b45184da4f9

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](#)