

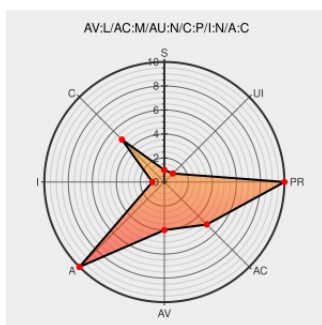


CVE-2011-1079

Published on: 06/21/2012 12:00:00 AM UTC

Last Modified on: 02/13/2023 04:29:00 AM UTC

CVE-2011-1079

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

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

The `bnep_sock_ioctl` function in `net/bluetooth/bnep/sock.c` in the Linux kernel before 2.6.39 does not ensure that a certain device field ends with a `'\0'` character, which allows local users to obtain potentially sensitive information from kernel stack memory, or cause a denial of service (BUG and system crash), via a `BNEPCONNADD` command.

CVE-2011-1079 has been assigned by secalert@redhat.com to track the vulnerability

CVSS2 Score: **5.4 - MEDIUM**

Access
Vector

LOCAL

Access
Complexity

MEDIUM

Authentication

NONE

Confidentiality
Impact

PARTIAL

Integrity
Impact

NONE

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=43629f8f5ea32a998d06d1bb41eefa0e821ff573](https://git.kernel.org/?p=linux/kernel/git/torvalds/linux-2.6.git%3Ba=commit%3Bh=43629f8f5ea32a998d06d1bb41eefa0e821ff573)

access.redhat.com

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

[REDHAT RHSA-2011:0833](#)

Bluetooth: bnep: fix buffer
overflow ·
torvalds/linux@43629f8 ·
GitHub

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

[CONFIRM](#)
github.com/torvalds/linux/commit/43629f8f5ea32a998d06d1bb41eefa0e821ff573

681260 – (CVE-2011-1079)

[bugzilla.redhat.com](#)

[CONFIRM](#) bugzilla.redhat.com/show_bug.cgi?id=681260

CVE-2011-1079 kernel: bnep device field missing NULL terminator	text/html	
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
Kernel Live Patch Security Notice LSN-0053-1 ~ Packet Storm	packetstormsecurity.com text/html	 MISC packetstormsecurity.com/files/153799/Kernel-Live-Patch-Security-Notice-LSN-0053-1.html
oss-security - Re: CVE request: kernel: two bluetooth and one ebttables infoleaks/DoSes	www.openwall.com text/html	 MLIST [oss-security] 20110301 Re: CVE request: kernel: two bluetooth and one ebttables infoleaks/DoSes
ASA-2011-208 (RHSA- 2011-0833)	downloads.avaya.com text/html	 CONFIRM downloads.avaya.com/css/P8/documents/100145416
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	2.6.38.3	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: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

[← Previous ID](#)

[Next ID→](#)

© 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](#)