



CVE-2013-6336

Published on: 11/04/2013 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:28:38 PM UTC

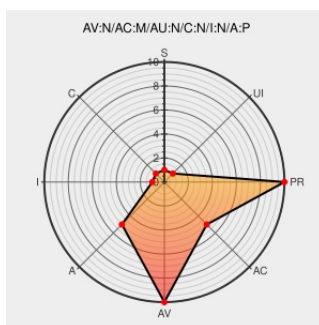
CVE-2013-6336

[Source: Mitre](#)

[Source: NIST](#)

[CVE.ORG](#)

[Print: PDF](#)



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

The `ieee802154_map_rec` function in `epan/dissectors/packet-ieee802154.c` in the IEEE 802.15.4 dissector in Wireshark 1.8.x before 1.8.11 and 1.10.x before 1.10.3 uses an incorrect pointer chain, which allows remote attackers to cause a denial of service (application crash) via a crafted packet.

CVE-2013-6336 has been assigned by [M](#) cve@mitre.org to track the vulnerability

CVSS2 Score: **4.3 - MEDIUM**

Access
Vector

NETWORK

Access
Complexity

MEDIUM

Authentication

NONE

Confidentiality
Impact

NONE

Integrity
Impact

NONE

Availability
Impact

PARTIAL

CVE References

Description

Tags

Link

code.wireshark Code Review -
wireshark.git/tree

[Patch](#)
[anonsvn.wireshark.org](#)
[text/xml](#)

[CONFIRM](#)
[anonsvn.wireshark.org/viewvc/trunk/epan/dissectors/packet-ieee802154.c?r1=52036&r2=52035&pathrev=52036](#)

9139 - Buildbot crash output: fuzz-
2013-09-12-20795.pcap

[Exploit](#)
[bugs.wireshark.org](#)
[text/html](#)

[CONFIRM](#) [bugs.wireshark.org/bugzilla/show_bug.cgi?id=9139](#)

code.wireshark Code Review -
wireshark.git/tree

[Patch](#)
[anonsvn.wireshark.org](#)
[text/xml](#)

[CONFIRM](#) [anonsvn.wireshark.org/viewvc?view=revision&revision=52036](#)

Repository / Oval Repository

[oval.cisecurity.org](#)
[text/html](#)

[OVAL](#) [oval:org.mitre.oval:def:19193](#)

openSUSE-SU-2013:16/1-1: moderate: update for wireshark	lists.opensuse.org text/html	 SUSE openSUSE-SU-2013:16/1
Debian -- Security Information -- DSA-2792-1 wireshark	www.debian.org Depreciated Link text/html	 DEBIAN DSA-2792
openSUSE-SU-2013:1675-1: moderate: update for wireshark	lists.opensuse.org text/html	 SUSE openSUSE-SU-2013:1675
Wireshark · wnpa-sec-2013-61 · IEEE 802.15.4 dissector crash	Vendor Advisory www.wireshark.org text/html	 CONFIRM www.wireshark.org/security/wnpa-sec-2013-61.html
Red Hat Customer Portal	web.archive.org text/html Inactive Link Not Archived	 REDHAT RHSA-2014:0342

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
Application	Wireshark	Wireshark	1.10.0	All	All	All
Application	Wireshark	Wireshark	1.10.1	All	All	All
Application	Wireshark	Wireshark	1.10.2	All	All	All
Application	Wireshark	Wireshark	1.8.0	All	All	All
Application	Wireshark	Wireshark	1.8.1	All	All	All
Application	Wireshark	Wireshark	1.8.10	All	All	All
Application	Wireshark	Wireshark	1.8.2	All	All	All
Application	Wireshark	Wireshark	1.8.3	All	All	All
Application	Wireshark	Wireshark	1.8.4	All	All	All
Application	Wireshark	Wireshark	1.8.5	All	All	All
Application	Wireshark	Wireshark	1.8.6	All	All	All
Application	Wireshark	Wireshark	1.8.7	All	All	All
Application	Wireshark	Wireshark	1.8.8	All	All	All
Application	Wireshark	Wireshark	1.8.9	All	All	All
Application	Wireshark	Wireshark	1.10.0	All	All	All
Application	Wireshark	Wireshark	1.10.1	All	All	All
Application	Wireshark	Wireshark	1.10.2	All	All	All
Application	Wireshark	Wireshark	1.8.0	All	All	All
Application	Wireshark	Wireshark	1.8.1	All	All	All

Application	Wireshark	Wireshark	1.8.10	All	All	All
Application	Wireshark	Wireshark	1.8.2	All	All	All
Application	Wireshark	Wireshark	1.8.3	All	All	All
Application	Wireshark	Wireshark	1.8.4	All	All	All
Application	Wireshark	Wireshark	1.8.5	All	All	All
Application	Wireshark	Wireshark	1.8.6	All	All	All
Application	Wireshark	Wireshark	1.8.7	All	All	All
Application	Wireshark	Wireshark	1.8.8	All	All	All
Application	Wireshark	Wireshark	1.8.9	All	All	All
cpe:2.3:a:wireshark:wireshark:1.10.0:*:*:*:*:*:						
cpe:2.3:a:wireshark:wireshark:1.10.1:*:*:*:*:*:						
cpe:2.3:a:wireshark:wireshark:1.10.2:*:*:*:*:*:						
cpe:2.3:a:wireshark:wireshark:1.8.0:*:*:*:*:*:						
cpe:2.3:a:wireshark:wireshark:1.8.1:*:*:*:*:*:						
cpe:2.3:a:wireshark:wireshark:1.8.10:*:*:*:*:*:						
cpe:2.3:a:wireshark:wireshark:1.8.2:*:*:*:*:*:						
cpe:2.3:a:wireshark:wireshark:1.8.3:*:*:*:*:*:						
cpe:2.3:a:wireshark:wireshark:1.8.4:*:*:*:*:*:						
cpe:2.3:a:wireshark:wireshark:1.8.5:*:*:*:*:*:						
cpe:2.3:a:wireshark:wireshark:1.8.6:*:*:*:*:*:						
cpe:2.3:a:wireshark:wireshark:1.8.7:*:*:*:*:*:						
cpe:2.3:a:wireshark:wireshark:1.8.8:*:*:*:*:*:						
cpe:2.3:a:wireshark:wireshark:1.8.9:*:*:*:*:*:						
cpe:2.3:a:wireshark:wireshark:1.10.0:*:*:*:*:*:						
cpe:2.3:a:wireshark:wireshark:1.10.1:*:*:*:*:*:						
cpe:2.3:a:wireshark:wireshark:1.10.2:*:*:*:*:*:						
cpe:2.3:a:wireshark:wireshark:1.8.0:*:*:*:*:*:						
cpe:2.3:a:wireshark:wireshark:1.8.1:*:*:*:*:*:						
cpe:2.3:a:wireshark:wireshark:1.8.10:*:*:*:*:*:						
cpe:2.3:a:wireshark:wireshark:1.8.2:*:*:*:*:*:						

cpe:2.3:a:wireshark:wireshark:1.8.3:*****:
cpe:2.3:a:wireshark:wireshark:1.8.4:*****:
cpe:2.3:a:wireshark:wireshark:1.8.5:*****:
cpe:2.3:a:wireshark:wireshark:1.8.6:*****:
cpe:2.3:a:wireshark:wireshark:1.8.7:*****:
cpe:2.3:a:wireshark:wireshark:1.8.8:*****:
cpe:2.3:a:wireshark:wireshark:1.8.9:*****:

No vendor comments have been submitted for this CVE

[← Previous ID](#)

[Next ID→](#)