



CVE-2013-6339

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

Last Modified on: 03/23/2021 11:28:37 PM UTC

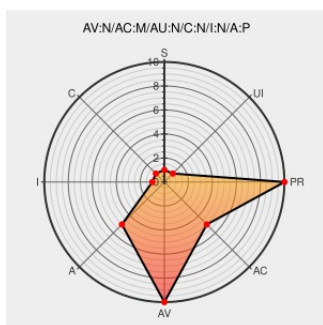
CVE-2013-6339

Source: Mitre

Source: NIST

CVE.ORG

Print: PDF



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

The dissect_openwire_type function in epan/dissectors/packet-openwire.c in the OpenWire dissector in Wireshark 1.8.x before 1.8.11 and 1.10.x before 1.10.3 allows remote attackers to cause a denial of service (loop) via a crafted packet.

CVE-2013-6339 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?view=revision&revision=52458](#)

9248 – Enabling the openwire protocol is leaking memory and crashes wireshark in few seconds with out of memory message

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

[CONFIRM](#) [bugs.wireshark.org/bugzilla/show_bug.cgi?id=9248](#)

code.wireshark Code Review - wireshark.git/tree

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

[CONFIRM](#) [anonsvn.wireshark.org/viewvc?view=revision&revision=52463](#)

Wireshark · wnpa-sec-2013-64 · ActiveMQ
OpenWire dissector large loop

[Vendor Advisory](#)
[www.wireshark.org](#)
[text/html](#)

[CONFIRM](#) [www.wireshark.org/security/wnpa-sec-2013-64.html](#)

openSUSE-SU-2013:1671-1: moderate: update

[lists.opensuse.org](#)

[SUSE](#) [openSUSE-SU-2013:1671](#)

for wireshark	text/html	
code.wireshark Code Review - wireshark.git/tree	Exploit Patch anonsvn.wireshark.org text/xml	 CONFIRM anonsvn.wireshark.org/viewvc/trunk/epan/dissectors/packet-openwire.c?r1=52463&r2=52462&pathrev=52463
code.wireshark Code Review - wireshark.git/tree	Patch anonsvn.wireshark.org text/xml	 CONFIRM anonsvn.wireshark.org/viewvc/trunk/epan/dissectors/packet-openwire.c?r1=52458&r2=52457&pathrev=52458
Repository / Oval Repository	oval.cisecurity.org text/html	 OVAL oval:org.mitre.oval:def:19086
openSUSE-SU-2013:1675-1: moderate: update for wireshark	lists.opensuse.org text/html	 SUSE openSUSE-SU-2013:1675
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→](#)