



CVE-2015-8711

Published on: 01/03/2016 12:00:00 AM UTC

Last Modified on: 11/07/2023 02:28:00 AM UTC

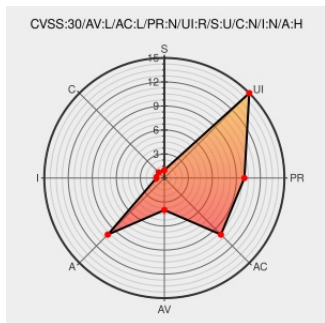
CVE-2015-8711

[Source: Mitre](#)

[Source: NIST](#)

[CVE.ORG](#)

[Print: PDF](#)



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

epan/dissectors/packet-nbap.c in the NBAP dissector in Wireshark 1.12.x before 1.12.9 and 2.0.x before 2.0.1 does not validate conversation data, which allows remote attackers to cause a denial of service (NULL pointer dereference and application crash) via a crafted packet.

CVE-2015-8711 has been assigned by [M](#) cve@mitre.org to track the vulnerability - currently rated as **MEDIUM** severity.

CVSS3 Score: **5.5 - MEDIUM**

Attack Vector	Attack Complexity	Privileges Required	User Interaction
LOCAL	LOW	NONE	REQUIRED
Scope	Confidentiality Impact	Integrity Impact	Availability Impact
UNCHANGED	NONE	NONE	HIGH

CVSS2 Score: **4.3 - MEDIUM**

Access Vector	Access Complexity	Authentication
NETWORK	MEDIUM	NONE
Confidentiality Impact	Integrity Impact	Availability Impact
NONE	NONE	PARTIAL

CVE References

Description	Tags	Link
Debian -- Security Information -- DSA-3505-1 wireshark	www.debian.org Deprecated Link text/html	@ DEBIAN DSA-3505

code.wireshark Code Review - wireshark.git/commit	code.wireshark.org text/xml	 CONFIRM code.wireshark.org/review/gitweb?p=wireshark.git;a=commit;h=5bf565690ad9f0771196d8fa237aa37fae3bb7cc
code.wireshark Code Review - wireshark.git/commit	code.wireshark.org text/xml	 CONFIRM code.wireshark.org/review/gitweb?p=wireshark.git;a=commit;h=5b4ada17723ed8af7e85cb48d537437ed614e417
Wireshark · wnpa-sec-2015-31 · NBAP dissector crashes	Vendor Advisory www.wireshark.org text/html	 CONFIRM www.wireshark.org/security/wnpa-sec-2015-31.html
Wireshark: Multiple vulnerabilities (GLSA 201604-05) — Gentoo security	security.gentoo.org text/html	 GENTOO GLSA-201604-05
code.wireshark Code Review - wireshark.git/commit	code.wireshark.org text/xml	 CONFIRM code.wireshark.org/review/gitweb?p=wireshark.git;a=commit;h=23379ae3624df82c170f48e5bb3250a97ec61c13
11841 – NBAP dissector crashes	bugs.wireshark.org text/html	 CONFIRM bugs.wireshark.org/bugzilla/show_bug.cgi?id=11841
Wireshark Multiple Denial of Service Vulnerabilities	cve.report (archive) text/html	 BID 79814
Wireshark Multiple Dissector/Parser Bugs Let Remote Users Deny Service - SecurityTracker	www.securitytracker.com text/html	 SECTRAK 1034551
11835 – Crash inside NBAP dissector	bugs.wireshark.org text/html	 CONFIRM bugs.wireshark.org/bugzilla/show_bug.cgi?id=11835
11602 – NBAP dissector crashes	bugs.wireshark.org text/html	 CONFIRM bugs.wireshark.org/bugzilla/show_bug.cgi?id=11602
Oracle Solaris Bulletin - January 2016	www.oracle.com text/html	 CONFIRM www.oracle.com/technetwork/topics/security/bulletinjan2016-2867206.html

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	1.12.0	All	All	All
Application	Wireshark	Wireshark	1.12.1	All	All	All
Application	Wireshark	Wireshark	1.12.2	All	All	All
Application	Wireshark	Wireshark	1.12.3	All	All	All
Application	Wireshark	Wireshark	1.12.4	All	All	All
Application	Wireshark	Wireshark	1.12.5	All	All	All
Application	Wireshark	Wireshark	1.12.6	All	All	All
Application	Wireshark	Wireshark	1.12.7	All	All	All
Application	Wireshark	Wireshark	1.12.8	All	All	All

Application	wireshark	wireshark	1.12.8	All	All	All
Application	Wireshark	Wireshark	2.0.0	All	All	All
Application	Wireshark	Wireshark	1.12.0	All	All	All
Application	Wireshark	Wireshark	1.12.1	All	All	All
Application	Wireshark	Wireshark	1.12.2	All	All	All
Application	Wireshark	Wireshark	1.12.3	All	All	All
Application	Wireshark	Wireshark	1.12.4	All	All	All
Application	Wireshark	Wireshark	1.12.5	All	All	All
Application	Wireshark	Wireshark	1.12.6	All	All	All
Application	Wireshark	Wireshark	1.12.7	All	All	All
Application	Wireshark	Wireshark	1.12.8	All	All	All
Application	Wireshark	Wireshark	2.0.0	All	All	All
cpe:2.3:a:wireshark:wireshark:1.12.0:****:*:*:						
cpe:2.3:a:wireshark:wireshark:1.12.1:****:*:*:						
cpe:2.3:a:wireshark:wireshark:1.12.2:****:*:*:						
cpe:2.3:a:wireshark:wireshark:1.12.3:****:*:*:						
cpe:2.3:a:wireshark:wireshark:1.12.4:****:*:*:						
cpe:2.3:a:wireshark:wireshark:1.12.5:****:*:*:						
cpe:2.3:a:wireshark:wireshark:1.12.6:****:*:*:						
cpe:2.3:a:wireshark:wireshark:1.12.7:****:*:*:						
cpe:2.3:a:wireshark:wireshark:1.12.8:****:*:*:						
cpe:2.3:a:wireshark:wireshark:2.0.0:****:*:*:						
cpe:2.3:a:wireshark:wireshark:1.12.0:****:*:*:						
cpe:2.3:a:wireshark:wireshark:1.12.1:****:*:*:						
cpe:2.3:a:wireshark:wireshark:1.12.2:****:*:*:						
cpe:2.3:a:wireshark:wireshark:1.12.3:****:*:*:						
cpe:2.3:a:wireshark:wireshark:1.12.4:****:*:*:						
cpe:2.3:a:wireshark:wireshark:1.12.5:****:*:*:						
cpe:2.3:a:wireshark:wireshark:1.12.6:****:*:*:						
cpe:2.3:a:wireshark:wireshark:1.12.7:****:*:*:						
cpe:2.3:a:wireshark:wireshark:1.12.8:****:*:*:						

cpe:2.3:a:wireshark:wireshark:2.0.0:*****:

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](#)