

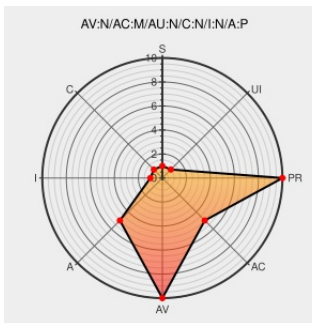


CVE-2015-7830

Published on: 11/14/2015 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:26:11 PM UTC

CVE-2015-7830

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

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

The pcapng_read_if_descr_block function in wiretap/pcapng.c in the pcapng parser in Wireshark 1.12.x before 1.12.8 uses too many levels of pointer indirection, which allows remote attackers to cause a denial of service (incorrect free and application crash) via a crafted packet that triggers interface-filter copying.

CVE-2015-7830 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

ZDI-15-624 | Zero Day Initiative

[www.zerodayinitiative.com](http://www.zerodayinitiative.com/text/html)
text/html

MISC www.zerodayinitiative.com/advisories/ZDI-15-624

Debian -- Security Information --
DSA-3505-1 wireshark

www.debian.org
Deprecated Link
text/html

DEBIAN DSA-3505

11455 -- Crash in multiple
binaries

[Issue Tracking](#)
[Vendor Advisory](#)
bugs.wireshark.org
text/html

CONFIRM bugs.wireshark.org/bugzilla/show_bug.cgi?id=11455

Wireshark · wnpa-sec-2015-30 ·
Pcapng file parser crash

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

CONFIRM www.wireshark.org/security/wnpa-sec-2015-30.html

Wireshark PCAPNG File CVE-2015-7830 Remote Code Execution Vulnerability	cve.report (archive) text/html	 BID 78723
Wireshark '/wiretap/pcapng.c' Remote Denial of Service Vulnerability	cve.report (archive) text/html	 BID 77101
Oracle Solaris Third Party Bulletin - October 2015	Third Party Advisory www.oracle.com text/html	 CONFIRM www.oracle.com/technetwork/topics/security/bulletinoct2015-2511968.html
Wireshark Bug in pcapng File Parser Lets Remote Users Cause the Target Service to Crash - SecurityTracker	www.securitytracker.com text/html	 SECTrack 1033953
code.wireshark Code Review - wireshark.git/commit	Patch code.wireshark.org text/xml	 CONFIRM code.wireshark.org/review/gitweb?p=wireshark.git;a=commit;h=72497918b16b706c3ba75e1f731f58b802ca14d1
openSUSE-SU-2015:1836-1: moderate: Security update for wireshark	lists.opensuse.org text/html	 SUSE openSUSE-SU-2015:1836

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	Oracle	Solaris	11.3	All	All	All
Operating System	Oracle	Solaris	11.3	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	1.12.0	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
cpe:2.3:o:oracle:solaris:11.3:*:*:*:*:*:						
cpe:2.3:o:oracle:solaris:11.3:*:*:*:*:*:						
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:1.12.0:*:*:*:*:*:						
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:*:*:*:*:*:						

No vendor comments have been submitted for this CVE

← Previous ID

Next ID →

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](#)