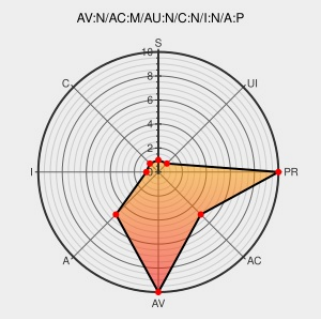
CVE-2015-6242

Published on: 08/24/2015 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:26:17 PM UTC

CVE-2015-6242

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF



Certain versions of Solaris from Oracle contain the following vulnerability:

The wmem_block_split_free_chunk function in epan/wmem/wmem_allocator_block.c in the wmem block allocator in the memory manager in Wireshark 1.12.x before 1.12.7 does not properly consider a certain case of multiple realloc operations that restore a memory chunk to its original size, which allows remote attackers to cause a denial of service (incorrect free operation and application crash) via a crafted packet.

CVE-2015-6242 has been assigned by cve@mitre.org to track the vulnerability

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
code.wireshark Code Review - wireshark.git/commit	code.wireshark.org, text/xml	CONFIRM code.wireshark.org/review/gitweb?p=wireshark.git;a=commit;h=eaf1aad31e7c0a4908c20a42ae118c4dc8d474b6
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 · wnpa-sec-2015-22 · Memory manager crash	Vendor Advisory, www.wireshark.org, text/html	CONFIRM www.wireshark.org/security/wnpa-sec-2015-22.html
Wireshark Dissector Bugs Lets	www.securitytracker.com	SECTRACK 1033272

Remote Users Cause the Target Service to Crash - SecurityTracker	text/html	
[SECURITY] Fedora 22 Update: wireshark-1.12.7-2.fc22	lists.fedoraproject.org text/html	FEDORA FEDORA-2015-13945
openSUSE-SU-2015:1836-1: moderate: Security update for wireshark	lists.opensuse.org text/html	SUSE openSUSE-SU-2015:1836
[SECURITY] Fedora 23 Update: wireshark-1.12.7-2.fc23	lists.fedoraproject.org text/html	FEDORA FEDORA-2015-13946
Bug 11373 – Decoding SOCKS packets crashes on Windows and Linux	Issue Tracking bugs.wireshark.org text/html	CONFIRM bugs.wireshark.org/bugzilla/show_bug.cgi?id=11373
Debian -- Security Information -- DSA-3367-1 wireshark	www.debian.org Depreciated Link text/html	DEBIAN DSA-3367

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	1.12.0	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

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:1.12.0:*:*:*:*:*:*:*

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:*:*:*:*:*:*:*

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→