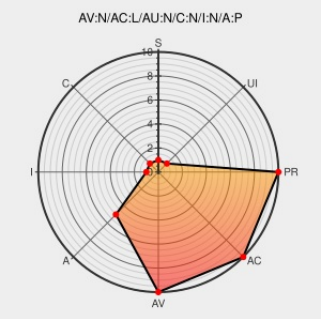
CVE-2014-6431

Published on: 09/20/2014 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:25:54 PM UTC

CVE-2014-6431

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



Certain versions of Wireshark from Wireshark contain the following vulnerability:

Buffer overflow in the SnifferDecompress function in wiretap/ngsniffer.c in the DOS Sniffer file parser in Wireshark 1.10.x before 1.10.10 and 1.12.x before 1.12.1 allows remote attackers to cause a denial of service (application crash) via a crafted file that triggers writes of uncompressed bytes beyond the end of the output buffer.

CVE-2014-6431 has been assigned by cve@mitre.org to track the vulnerability

CVSS2 Score: 5 - MEDIUM

Access Vector	Access Complexity	Authentication
NETWORK	LOW	NONE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
NONE	NONE	PARTIAL

CVE References

Description	Tags	Link
About Secunia Research | Flexera	secunia.com, Depreciated Link, text/html	SECUNIA 60280
Wireshark · wnpa-sec-2014-19 · Sniffer file parser crash	www.wireshark.org, text/html	CONFIRM www.wireshark.org/security/wnpa-sec-2014-19.html
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=47c592938ba9f0caeacc4c2ccadb370e72f293a2
Bug 10461 – invalid memory accesses in the SnifferDecompress function	bugs.wireshark.org, text/html	CONFIRM bugs.wireshark.org/bugzilla/show_bug.cgi?id=10461

404 Not Found	linux.oracle.com text/html Inactive Link Not Archived	CONFIRM linux.oracle.com/errata/ELSA-2014-1676
Red Hat Customer Portal	web.archive.org text/html Inactive Link Not Archived	REDHAT RHSA-2014:1676
[security-announce] SUSE-SU-2014:1221-1: important: Security update for	lists.opensuse.org text/html	SUSE SUSE-SU-2014:1221
Security Advisory SA61933 - Oracle Linux update for wireshark - Secunia	web.archive.org text/html	SECUNIA 61933
Red Hat Customer Portal	web.archive.org text/html Inactive Link Not Archived	REDHAT RHSA-2014:1677
404 Not Found	linux.oracle.com text/html Inactive Link Not Archived	CONFIRM linux.oracle.com/errata/ELSA-2014-1677
Debian -- Security Information -- DSA-3049-1 wireshark	www.debian.org Depreciated Link text/html	DEBIAN DSA-3049
About Secunia Research | Flexera	secunia.com Depreciated Link text/html	SECUNIA 60578
openSUSE-SU-2014:1249-1: moderate: wireshark: update to 1.10.10 security	lists.opensuse.org text/html	SUSE openSUSE-SU-2014:1249
Security Advisory SA61929 - Oracle Linux update for wireshark - Secunia	web.archive.org text/html	SECUNIA 61929

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	1.10.3	All	All	All
Application	Wireshark	Wireshark	1.10.4	All	All	All
Application	Wireshark	Wireshark	1.10.5	All	All	All
Application	Wireshark	Wireshark	1.10.6	All	All	All

Application	Wireshark	Wireshark	1.10.7	All	All	All
Application	Wireshark	Wireshark	1.10.8	All	All	All
Application	Wireshark	Wireshark	1.10.9	All	All	All
Application	Wireshark	Wireshark	1.12.0	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	1.10.3	All	All	All
Application	Wireshark	Wireshark	1.10.4	All	All	All
Application	Wireshark	Wireshark	1.10.5	All	All	All
Application	Wireshark	Wireshark	1.10.6	All	All	All
Application	Wireshark	Wireshark	1.10.7	All	All	All
Application	Wireshark	Wireshark	1.10.8	All	All	All
Application	Wireshark	Wireshark	1.10.9	All	All	All
Application	Wireshark	Wireshark	1.12.0	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:1.10.3:*:*:*:*:*:*:*:

cpe:2.3:a:wireshark:wireshark:1.10.4:*:*:*:*:*:*:*:

cpe:2.3:a:wireshark:wireshark:1.10.5:*:*:*:*:*:*:*:

cpe:2.3:a:wireshark:wireshark:1.10.6:*:*:*:*:*:*:*:

cpe:2.3:a:wireshark:wireshark:1.10.7:*:*:*:*:*:*:*:

cpe:2.3:a:wireshark:wireshark:1.10.8:*:*:*:*:*:*:*:

cpe:2.3:a:wireshark:wireshark:1.10.9:*:*:*:*:*:*:*:

cpe:2.3:a:wireshark:wireshark:1.12.0:*:*:*:*:*:*:*:

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:1.10.3:*:*:*:*:*:*:*:

cpe:2.3:a:wireshark:wireshark:1.10.4:*:*:*:*:*:*:*:

cpe:2.3:a:wireshark:wireshark:1.10.5:*:*:*:*:*:*:*

cpe:2.3:a:wireshark:wireshark:1.10.6:*:*:*:*:*:*:*

cpe:2.3:a:wireshark:wireshark:1.10.7:*:*:*:*:*:*:*

cpe:2.3:a:wireshark:wireshark:1.10.8:*:*:*:*:*:*:*

cpe:2.3:a:wireshark:wireshark:1.10.9:*:*:*:*:*:*:*

cpe:2.3:a:wireshark:wireshark:1.12.0:*:*:*:*:*:*:*

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→