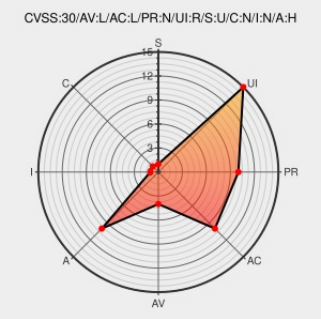
CVE-2015-8736

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

Last Modified on: 03/23/2021 11:26:14 PM UTC

CVE-2015-8736

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



Certain versions of Wireshark from Wireshark contain the following vulnerability:

The mp2t_find_next_pcr function in wiretap/mp2t.c in the MP2T file parser in Wireshark 2.0.x before 2.0.1 does not reserve memory for a trailer, which allows remote attackers to cause a denial of service (stack-based buffer overflow and application crash) via a crafted file.

CVE-2015-8736 has been assigned by 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
Wireshark · wnpa-sec-2015-54 · MP2T file parser crash	Vendor Advisory, www.wireshark.org, text/html	CONFIRM www.wireshark.org/security/wnpa-sec-2015-54.html
Wireshark: Multiple vulnerabilities (GLSA	security.gentoo.org	GENTOO GLSA-201604-05

201604-05) — Gentoo security	text/html	
Wireshark Multiple Security Vulnerabilities	cve.report (archive) text/html	BID 79382
Bug 11820 – Wireshark stack-based buffer overflow in file_read (wtap_read_bytes_or_eof/mp2t_find_next_pcr)	bugs.wireshark.org text/html	CONFIRM bugs.wireshark.org/bugzilla/show_bug.cgi?id=1182(
code.wireshark Code Review - wireshark.git/commit	code.wireshark.org text/xml	CONFIRM code.wireshark.org/review/gitweb?p=wireshark.git;a=commit;h=baa3eab78b422616a92ee38551c1b1
Wireshark Multiple Dissector/Parser Bugs Let Remote Users Deny Service - SecurityTracker	www.securitytracker.com text/html	SECTRACK 1034551

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	2.0.0	All	All	All
Application	Wireshark	Wireshark	2.0.0	All	All	All

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

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

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→