

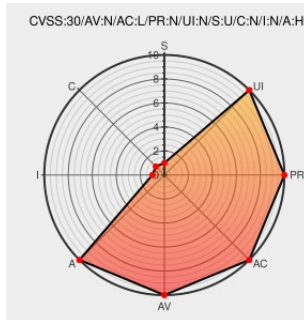


CVE-2017-11410

Published on: 07/18/2017 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:26:24 PM UTC

CVE-2017-11410

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

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

In Wireshark through 2.0.13 and 2.2.x through 2.2.7, the WBXML dissector could go into an infinite loop, triggered by packet injection or a malformed capture file. This was addressed in epan/dissectors/packet-wbxml.c by adding validation of the relationships between indexes and lengths. NOTE: this vulnerability exists because of an incomplete fix for CVE-2017-7702.

CVE-2017-11410 has been assigned by [M](#) cve@mitre.org to track the vulnerability - currently rated as **HIGH** severity.

CVSS3 Score: **7.5 - HIGH**

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

CVSS2 Score: **7.8 - HIGH**

Access Vector	Access Complexity	Authentication
NETWORK	LOW	NONE
Confidentiality Impact	Integrity Impact	Availability Impact
NONE	NONE	COMPLETE

CVE References

Description	Tags	Link
Wireshark · wnpa-sec-2017-13 · WBXML dissector infinite loop	Vendor Advisory www.wireshark.org	CONFIRM www.wireshark.org/security/wnpa-sec-2017-13.html

[text/html](#)

13796 – Buildbot crash output: fuzz-2017-06-12-4268.pcap

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

 [CONFIRM bugs.wireshark.org/bugzilla/show_bug.cgi?id=13796](https://bugs.wireshark.org/bugzilla/show_bug.cgi?id=13796)

code.wireshark Code Review - wireshark.git/commit

[Issue Tracking](#)[Patch](#)[Vendor Advisory](#)[code.wireshark.org](#)[text/xml](#)

 [CONFIRM code.wireshark.org/review/gitweb?p=wireshark.git;a=commit;h=3c7168cc5f044b4da8747d35da0b2b204dabf398](https://code.wireshark.org/review/gitweb?p=wireshark.git;a=commit;h=3c7168cc5f044b4da8747d35da0b2b204dabf398)

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	2.0.1	All	All	All
Application	Wireshark	Wireshark	2.0.10	All	All	All
Application	Wireshark	Wireshark	2.0.11	All	All	All
Application	Wireshark	Wireshark	2.0.12	All	All	All
Application	Wireshark	Wireshark	2.0.13	All	All	All
Application	Wireshark	Wireshark	2.0.2	All	All	All
Application	Wireshark	Wireshark	2.0.3	All	All	All
Application	Wireshark	Wireshark	2.0.4	All	All	All
Application	Wireshark	Wireshark	2.0.5	All	All	All
Application	Wireshark	Wireshark	2.0.6	All	All	All
Application	Wireshark	Wireshark	2.0.7	All	All	All
Application	Wireshark	Wireshark	2.0.8	All	All	All
Application	Wireshark	Wireshark	2.0.9	All	All	All
Application	Wireshark	Wireshark	2.2.0	All	All	All
Application	Wireshark	Wireshark	2.2.1	All	All	All
Application	Wireshark	Wireshark	2.2.2	All	All	All
Application	Wireshark	Wireshark	2.2.3	All	All	All
Application	Wireshark	Wireshark	2.2.4	All	All	All
Application	Wireshark	Wireshark	2.2.5	All	All	All

Application	Wireshark	Wireshark	2.2.6	All	All	All
Application	Wireshark	Wireshark	2.2.7	All	All	All
Application	Wireshark	Wireshark	2.0.0	All	All	All
Application	Wireshark	Wireshark	2.0.1	All	All	All
Application	Wireshark	Wireshark	2.0.10	All	All	All
Application	Wireshark	Wireshark	2.0.11	All	All	All
Application	Wireshark	Wireshark	2.0.12	All	All	All
Application	Wireshark	Wireshark	2.0.13	All	All	All
Application	Wireshark	Wireshark	2.0.2	All	All	All
Application	Wireshark	Wireshark	2.0.3	All	All	All
Application	Wireshark	Wireshark	2.0.4	All	All	All
Application	Wireshark	Wireshark	2.0.5	All	All	All
Application	Wireshark	Wireshark	2.0.6	All	All	All
Application	Wireshark	Wireshark	2.0.7	All	All	All
Application	Wireshark	Wireshark	2.0.8	All	All	All
Application	Wireshark	Wireshark	2.0.9	All	All	All
Application	Wireshark	Wireshark	2.2.0	All	All	All
Application	Wireshark	Wireshark	2.2.1	All	All	All
Application	Wireshark	Wireshark	2.2.2	All	All	All
Application	Wireshark	Wireshark	2.2.3	All	All	All
Application	Wireshark	Wireshark	2.2.4	All	All	All
Application	Wireshark	Wireshark	2.2.5	All	All	All
Application	Wireshark	Wireshark	2.2.6	All	All	All
Application	Wireshark	Wireshark	2.2.7	All	All	All
cpe:2.3:a:wireshark:wireshark:2.0.0:*:*:*:*:*:						
cpe:2.3:a:wireshark:wireshark:2.0.1:*:*:*:*:*:						
cpe:2.3:a:wireshark:wireshark:2.0.10:*:*:*:*:*:						
cpe:2.3:a:wireshark:wireshark:2.0.11:*:*:*:*:*:						
cpe:2.3:a:wireshark:wireshark:2.0.12:*:*:*:*:*:						
cpe:2.3:a:wireshark:wireshark:2.0.13:*:*:*:*:*:						
cpe:2.3:a:wireshark:wireshark:2.0.2:*:*:*:*:*:						
cpe:2.3:a:wireshark:wireshark:2.0.3:*:*:*:*:*:						
cpe:2.3:a:wireshark:wireshark:2.0.4:*:*:*:*:*:						

cpe:2.3:a:wireshark:wireshark:2.0.5:~::~::~:
cpe:2.3:a:wireshark:wireshark:2.0.6:~::~::~:
cpe:2.3:a:wireshark:wireshark:2.0.7:~::~::~:
cpe:2.3:a:wireshark:wireshark:2.0.8:~::~::~:
cpe:2.3:a:wireshark:wireshark:2.0.9:~::~::~:
cpe:2.3:a:wireshark:wireshark:2.2.0:~::~::~:
cpe:2.3:a:wireshark:wireshark:2.2.1:~::~::~:
cpe:2.3:a:wireshark:wireshark:2.2.2:~::~::~:
cpe:2.3:a:wireshark:wireshark:2.2.3:~::~::~:
cpe:2.3:a:wireshark:wireshark:2.2.4:~::~::~:
cpe:2.3:a:wireshark:wireshark:2.2.5:~::~::~:
cpe:2.3:a:wireshark:wireshark:2.2.6:~::~::~:
cpe:2.3:a:wireshark:wireshark:2.2.7:~::~::~:
cpe:2.3:a:wireshark:wireshark:2.0.0:~::~::~:
cpe:2.3:a:wireshark:wireshark:2.0.1:~::~::~:
cpe:2.3:a:wireshark:wireshark:2.0.10:~::~::~:
cpe:2.3:a:wireshark:wireshark:2.0.11:~::~::~:
cpe:2.3:a:wireshark:wireshark:2.0.12:~::~::~:
cpe:2.3:a:wireshark:wireshark:2.0.13:~::~::~:
cpe:2.3:a:wireshark:wireshark:2.0.2:~::~::~:
cpe:2.3:a:wireshark:wireshark:2.0.3:~::~::~:
cpe:2.3:a:wireshark:wireshark:2.0.4:~::~::~:
cpe:2.3:a:wireshark:wireshark:2.0.5:~::~::~:
cpe:2.3:a:wireshark:wireshark:2.0.6:~::~::~:
cpe:2.3:a:wireshark:wireshark:2.0.7:~::~::~:
cpe:2.3:a:wireshark:wireshark:2.0.8:~::~::~:
cpe:2.3:a:wireshark:wireshark:2.0.9:~::~::~:
cpe:2.3:a:wireshark:wireshark:2.2.0:~::~::~:
cpe:2.3:a:wireshark:wireshark:2.2.1:~::~::~:

cpe:2.3:a:wireshark:wireshark:2.2.2:*****:
cpe:2.3:a:wireshark:wireshark:2.2.3:*****:
cpe:2.3:a:wireshark:wireshark:2.2.4:*****:
cpe:2.3:a:wireshark:wireshark:2.2.5:*****:
cpe:2.3:a:wireshark:wireshark:2.2.6:*****:
cpe:2.3:a:wireshark:wireshark:2.2.7:*****:

No vendor comments have been submitted for this CVE

[← Previous ID](#)

[Next ID→](#)