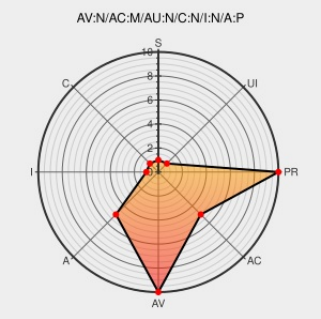
# CVE-2014-4020

Published on: 06/18/2014 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:25:43 PM UTC

## CVE-2014-4020

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




Certain versions of Wireshark from Wireshark contain the following vulnerability:

The dissect_frame function in epan/dissectors/packet-frame.c in the frame metadissector in Wireshark 1.10.x before 1.10.8 interprets a negative integer as a length value even though it was intended to represent an error condition, which allows remote attackers to cause a denial of service (application crash) via a crafted packet.

CVE-2014-4020 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 | Patch, code.wireshark.org, text/xml | CONFIRM code.wireshark.org/review/gitweb?p=wireshark.git;a=commit;h=beb119f911a698d44f4baa06d888bb1e775983bc |
| openSUSE-SU-2014:0836-1: wireshark: Fix for possible DoS | lists.opensuse.org, text/html | SUSE openSUSE-SU-2014:0836 |
| Wireshark · wnpa-sec-2014-07 · Frame metadissector crash. | Vendor Advisory, www.wireshark.org, text/html | CONFIRM www.wireshark.org/security/wnpa-sec-2014-07.html |
| 10030 – Buildbot crash output: fuzz-2014-04-23-25489.pcap | Exploit, bugs.wireshark.org, text/html | CONFIRM bugs.wireshark.org/bugzilla/show_bug.cgi?id=10030 |

| | | |
|---|---|---|
| Bug 9999 – Buildbot crash output: randpkt-2014-04-17-16318.pcap | Exploit<br>bugs.wireshark.org<br>text/html | CONFIRM bugs.wireshark.org/bugzilla/show_bug.cgi?id=9999 |



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 | 1.10.0 | 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 |

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:1.10.0:*:*:*:*:*:*:*

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

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→