



# CVE-2012-6058

Published on: 12/05/2012 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:28:22 PM UTC

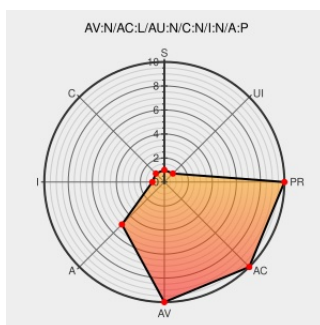
## CVE-2012-6058

[Source: Mitre](#)

[Source: NIST](#)

[CVE.ORG](#)

[Print: PDF](#)



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

Integer overflow in the dissect\_icmpv6 function in epan/dissectors/packet-icmpv6.c in the ICMPv6 dissector in Wireshark 1.6.x before 1.6.12 and 1.8.x before 1.8.4 allows remote attackers to cause a denial of service (infinite loop) via a crafted Number of Sources value.

CVE-2012-6058 has been assigned by [M](#) cve@mitre.org to track the vulnerability

CVSS2 Score: **5 - MEDIUM**

**Access Vector**

**NETWORK**

**Access Complexity**

**LOW**

**Authentication**

**NONE**

**Confidentiality Impact**

**NONE**

**Integrity Impact**

**NONE**

**Availability Impact**

**PARTIAL**

## CVE References

**Description**

**Tags**

**Link**

openSUSE-SU-2013:0151-1:  
moderate: wireshark to 1.8.4

[lists.opensuse.org](#)  
[text/html](#)

[SUSE openSUSE-SU-2013:0151](#)

7844 – Buildbot crash output: fuzz-  
2012-10-10-4301.pcap

[Exploit](#)  
[bugs.wireshark.org](#)  
[text/html](#)

[CONFIRM bugs.wireshark.org/bugzilla/show\\_bug.cgi?id=7844](#)

code.wireshark Code Review -  
wireshark.git/tree

[Exploit](#)  
[anonsvn.wireshark.org](#)  
[text/xml](#)

[CONFIRM anonsvn.wireshark.org/viewvc/trunk/epan/dissectors/packet-icmpv6.c?r1=45459&r2=45458&pathrev=45459](#)

Wireshark · wnpa-sec-2012-40

[Vendor Advisory](#)  
[www.wireshark.org](#)  
[text/html](#)

[CONFIRM www.wireshark.org/security/wnpa-sec-2012-40.html](#)

code.wireshark Code Review -  
wireshark.git/tree

[anonsvn.wireshark.org](https://anonsvn.wireshark.org)  
text/xml

 [CONFIRM anonsvn.wireshark.org/viewvc/?view=revision&revision=45459](https://anonsvn.wireshark.org/viewvc/?view=revision&revision=45459)

openSUSE-SU-2012:1633-1:  
moderate: wireshark to 1.8.4

[lists.opensuse.org](https://lists.opensuse.org)  
text/html

 [SUSE openSUSE-SU-2012:1633](https://openSUSE-SU-2012:1633)

Repository / Oval Repository

[oval.cisecurity.org](https://oval.cisecurity.org)  
text/html

 [OVAL oval.mitre.org/oval:def:16075](https://oval.mitre.org/oval:def:16075)

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](mailto: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 | <a href="#">Wireshark</a> | <a href="#">Wireshark</a> | 1.6.0   | All    | All     | All      |
| Application | <a href="#">Wireshark</a> | <a href="#">Wireshark</a> | 1.6.1   | All    | All     | All      |
| Application | <a href="#">Wireshark</a> | <a href="#">Wireshark</a> | 1.6.10  | All    | All     | All      |
| Application | <a href="#">Wireshark</a> | <a href="#">Wireshark</a> | 1.6.11  | All    | All     | All      |
| Application | <a href="#">Wireshark</a> | <a href="#">Wireshark</a> | 1.6.2   | All    | All     | All      |
| Application | <a href="#">Wireshark</a> | <a href="#">Wireshark</a> | 1.6.3   | All    | All     | All      |
| Application | <a href="#">Wireshark</a> | <a href="#">Wireshark</a> | 1.6.4   | All    | All     | All      |
| Application | <a href="#">Wireshark</a> | <a href="#">Wireshark</a> | 1.6.5   | All    | All     | All      |
| Application | <a href="#">Wireshark</a> | <a href="#">Wireshark</a> | 1.6.6   | All    | All     | All      |
| Application | <a href="#">Wireshark</a> | <a href="#">Wireshark</a> | 1.6.7   | All    | All     | All      |
| Application | <a href="#">Wireshark</a> | <a href="#">Wireshark</a> | 1.6.8   | All    | All     | All      |
| Application | <a href="#">Wireshark</a> | <a href="#">Wireshark</a> | 1.6.9   | All    | All     | All      |
| Application | <a href="#">Wireshark</a> | <a href="#">Wireshark</a> | 1.8.0   | All    | All     | All      |
| Application | <a href="#">Wireshark</a> | <a href="#">Wireshark</a> | 1.8.1   | All    | All     | All      |
| Application | <a href="#">Wireshark</a> | <a href="#">Wireshark</a> | 1.8.2   | All    | All     | All      |
| Application | <a href="#">Wireshark</a> | <a href="#">Wireshark</a> | 1.8.3   | All    | All     | All      |
| Application | <a href="#">Wireshark</a> | <a href="#">Wireshark</a> | 1.6.0   | All    | All     | All      |
| Application | <a href="#">Wireshark</a> | <a href="#">Wireshark</a> | 1.6.1   | All    | All     | All      |
| Application | <a href="#">Wireshark</a> | <a href="#">Wireshark</a> | 1.6.10  | All    | All     | All      |
| Application | <a href="#">Wireshark</a> | <a href="#">Wireshark</a> | 1.6.11  | All    | All     | All      |
| Application | <a href="#">Wireshark</a> | <a href="#">Wireshark</a> | 1.6.2   | All    | All     | All      |
| Application | <a href="#">Wireshark</a> | <a href="#">Wireshark</a> | 1.6.3   | All    | All     | All      |
| Application | <a href="#">Wireshark</a> | <a href="#">Wireshark</a> | 1.6.4   | All    | All     | All      |

|             |           |           |       |     |     |     |
|-------------|-----------|-----------|-------|-----|-----|-----|
| Application | Wireshark | Wireshark | 1.6.5 | All | All | All |
| Application | Wireshark | Wireshark | 1.6.6 | All | All | All |
| Application | Wireshark | Wireshark | 1.6.7 | All | All | All |
| Application | Wireshark | Wireshark | 1.6.8 | All | All | All |
| Application | Wireshark | Wireshark | 1.6.9 | All | All | All |
| Application | Wireshark | Wireshark | 1.8.0 | All | All | All |
| Application | Wireshark | Wireshark | 1.8.1 | All | All | All |
| Application | Wireshark | Wireshark | 1.8.2 | All | All | All |
| Application | Wireshark | Wireshark | 1.8.3 | All | All | All |

|                                                 |
|-------------------------------------------------|
| cpe:2.3:a:wireshark:wireshark:1.6.0:*:*:*:*:*:  |
| cpe:2.3:a:wireshark:wireshark:1.6.1:*:*:*:*:*:  |
| cpe:2.3:a:wireshark:wireshark:1.6.10:*:*:*:*:*: |
| cpe:2.3:a:wireshark:wireshark:1.6.11:*:*:*:*:*: |
| cpe:2.3:a:wireshark:wireshark:1.6.2:*:*:*:*:*:  |
| cpe:2.3:a:wireshark:wireshark:1.6.3:*:*:*:*:*:  |
| cpe:2.3:a:wireshark:wireshark:1.6.4:*:*:*:*:*:  |
| cpe:2.3:a:wireshark:wireshark:1.6.5:*:*:*:*:*:  |
| cpe:2.3:a:wireshark:wireshark:1.6.6:*:*:*:*:*:  |
| cpe:2.3:a:wireshark:wireshark:1.6.7:*:*:*:*:*:  |
| cpe:2.3:a:wireshark:wireshark:1.6.8:*:*:*:*:*:  |
| cpe:2.3:a:wireshark:wireshark:1.6.9:*:*:*:*:*:  |
| cpe:2.3:a:wireshark:wireshark:1.8.0:*:*:*:*:*:  |
| cpe:2.3:a:wireshark:wireshark:1.8.1:*:*:*:*:*:  |
| cpe:2.3:a:wireshark:wireshark:1.8.2:*:*:*:*:*:  |
| cpe:2.3:a:wireshark:wireshark:1.8.3:*:*:*:*:*:  |
| cpe:2.3:a:wireshark:wireshark:1.6.0:*:*:*:*:*:  |
| cpe:2.3:a:wireshark:wireshark:1.6.1:*:*:*:*:*:  |
| cpe:2.3:a:wireshark:wireshark:1.6.10:*:*:*:*:*: |
| cpe:2.3:a:wireshark:wireshark:1.6.11:*:*:*:*:*: |
| cpe:2.3:a:wireshark:wireshark:1.6.2:*:*:*:*:*:  |

|                                            |
|--------------------------------------------|
| cpe:2.3:a:wireshark:wireshark:1.6.3:*****: |
| cpe:2.3:a:wireshark:wireshark:1.6.4:*****: |
| cpe:2.3:a:wireshark:wireshark:1.6.5:*****: |
| cpe:2.3:a:wireshark:wireshark:1.6.6:*****: |
| cpe:2.3:a:wireshark:wireshark:1.6.7:*****: |
| cpe:2.3:a:wireshark:wireshark:1.6.8:*****: |
| cpe:2.3:a:wireshark:wireshark:1.6.9:*****: |
| cpe:2.3:a:wireshark:wireshark:1.8.0:*****: |
| cpe:2.3:a:wireshark:wireshark:1.8.1:*****: |
| cpe:2.3:a:wireshark:wireshark:1.8.2:*****: |
| cpe:2.3:a:wireshark:wireshark:1.8.3:*****: |

No vendor comments have been submitted for this CVE

[← Previous ID](#)

[Next ID→](#)