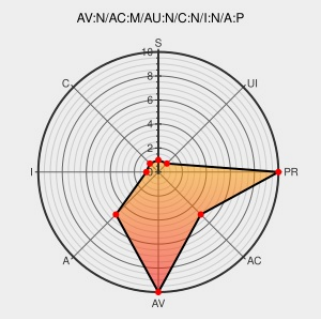
# CVE-2008-6472

Published on: 03/14/2009 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:25:17 PM UTC

## CVE-2008-6472

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




Certain versions of Wireshark from Wireshark contain the following vulnerability:

The WLCCP dissector in Wireshark 0.99.7 through 1.0.4 allows remote attackers to cause a denial of service (infinite loop) via unspecified vectors.

CVE-2008-6472 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 |
|---|---|---|
| Repository / Oval Repository | oval.cisecurity.org<br>text/html | OVAL<br>oval:org.mitre.oval:def:6223 |
| Support / Security / Advisories / / MDVSA-2008:242 \| Mandriva | www.mandriva.com<br>text/html | MANDRIVA MDVSA-2008:242 |
| Wireshark SMTP Processing Denial of Service Vulnerability - Secunia Advisories - Vulnerability Intelligence - Secunia.com | Vendor Advisory<br>web.archive.org<br>text/html | SECUNIA 32840 |
| Wireshark: wnpa-sec-2008-07 | Patch<br>Vendor Advisory<br>www.wireshark.org<br>text/xml | CONFIRM<br>www.wireshark.org/security/wnpa-sec-2008-07.html |
| Support | www.redhat.com<br>text/html | REDHAT RHSA-2009:0313 |

| | | |
|---|---|---|
| Repository / Oval Repository | oval.cisecurity.org<br>text/html | OVAL<br>oval:org.mitre.oval:def:9629 |
| IBM X-Force Exchange | exchange.xforce.ibmcloud.com<br>text/html | XF wireshark-wlccp-dos(47292) |
| Security Alerts - Secunia | web.archive.org<br>text/html | SECUNIA 34144 |



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 | 0.99.7 | All | All | All |
| Application | Wireshark | Wireshark | 0.99.8 | All | All | All |
| Application | Wireshark | Wireshark | 1.0 | All | All | All |
| Application | Wireshark | Wireshark | 1.0.0 | All | All | All |
| Application | Wireshark | Wireshark | 1.0.1 | All | All | All |
| Application | Wireshark | Wireshark | 1.0.2 | All | All | All |
| Application | Wireshark | Wireshark | 1.0.3 | All | All | All |
| Application | Wireshark | Wireshark | 1.0.4 | All | All | All |
| Application | Wireshark | Wireshark | 0.99.7 | All | All | All |
| Application | Wireshark | Wireshark | 0.99.8 | All | All | All |
| Application | Wireshark | Wireshark | 1.0 | All | All | All |
| Application | Wireshark | Wireshark | 1.0.0 | All | All | All |
| Application | Wireshark | Wireshark | 1.0.1 | All | All | All |
| Application | Wireshark | Wireshark | 1.0.2 | All | All | All |
| Application | Wireshark | Wireshark | 1.0.3 | All | All | All |
| Application | Wireshark | Wireshark | 1.0.4 | All | All | All |

cpe:2.3:a:wireshark:wireshark:0.99.7:*:*:*:*:*:*:*:

cpe:2.3:a:wireshark:wireshark:0.99.8:*:*:*:*:*:*:*:

cpe:2.3:a:wireshark:wireshark:1.0:*:*:*:*:*:*:*:

cpe:2.3:a:wireshark:wireshark:1.0.0:*:*:*:*:*:*:*:

cpe:2.3:a:wireshark:wireshark:1.0.1:*:*:*:*:*:*:*:

cpe:2.3:a:wireshark:wireshark:1.0.2:*:*:*:*:*:*:*

cpe:2.3:a:wireshark:wireshark:1.0.3:*:*:*:*:*:*:*

cpe:2.3:a:wireshark:wireshark:1.0.4:*:*:*:*:*:*:*

cpe:2.3:a:wireshark:wireshark:0.99.7:*:*:*:*:*:*:*

cpe:2.3:a:wireshark:wireshark:0.99.8:*:*:*:*:*:*:*

cpe:2.3:a:wireshark:wireshark:1.0:*:*:*:*:*:*:*

cpe:2.3:a:wireshark:wireshark:1.0.0:*:*:*:*:*:*:*

cpe:2.3:a:wireshark:wireshark:1.0.1:*:*:*:*:*:*:*

cpe:2.3:a:wireshark:wireshark:1.0.2:*:*:*:*:*:*:*

cpe:2.3:a:wireshark:wireshark:1.0.3:*:*:*:*:*:*:*

cpe:2.3:a:wireshark:wireshark:1.0.4:*:*:*:*:*:*:*

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→