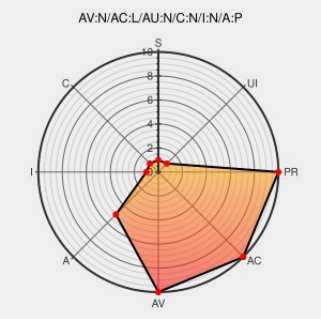
# CVE-2010-2992

Published on: 08/13/2010 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:23:10 PM UTC

## CVE-2010-2992

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




Certain versions of Wireshark from Wireshark contain the following vulnerability:

packet-gsm_a_rr.c in the GSM A RR dissector in Wireshark 1.2.2 through 1.2.9 allows remote attackers to cause a denial of service (crash) via unknown vectors that trigger a NULL pointer dereference.

CVE-2010-2992 has been assigned by cve@mitre.org to track the vulnerability

### CVSS2 Score: 5 - MEDIUM

| Access Vector | Access Complexity | Authentication |
|---|---|---|
| NETWORK | LOW | NONE |
| **Confidentiality Impact** | **Integrity Impact** | **Availability Impact** |
| NONE | NONE | PARTIAL |

### CVE References

| Description | Tags | Link |
|---|---|---|
| Webmail : Solution de messagerie professionnelle - OVHcloud- OVH | www.vupen.com text/html | VUPEN ADV-2011-0212 |
| Wireshark · Wireshark 1.2.10 Release Notes | Vendor Advisory www.wireshark.org text/html | CONFIRM www.wireshark.org/docs/relnotes/wireshark-1.2.10.html |
| [security-announce] SUSE Security Summary Report: SUSE-SR:2011:001 | lists.opensuse.org text/html | SUSE SUSE-SR:2011:001 |
| Webmail : Solution de messagerie professionnelle - OVHcloud- OVH | www.vupen.com text/html | VUPEN ADV-2011-0076 |
| 4897 – Buildbot crash output: fuzz-2010-06-20-7873.pcap | bugs.wireshark.org text/html | CONFIRM bugs.wireshark.org/bugzilla/show_bug.cgi?id=4897 |
| SUSE update for multiple packages - Advisories - Community | web.archive.org | SECUNIA 42877 |

| | | |
|---|---|---|
| | text/html | |
| [security-announce] SUSE Security Summary Report: SUSE-SR:2011:002 | lists.opensuse.org<br>text/html | SUSE SUSE-SR:2011:002 |
| SUSE update for Multiple Packages - Secunia.com | web.archive.org<br>text/html | SECUNIA 43068 |
| Repository / Oval Repository | oval.cisecurity.org<br>text/html | OVAL oval:org.mitre.oval:def:11651 |



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 | 1.2.2 | All | All | All |
| Application | Wireshark | Wireshark | 1.2.3 | All | All | All |
| Application | Wireshark | Wireshark | 1.2.4 | All | All | All |
| Application | Wireshark | Wireshark | 1.2.5 | All | All | All |
| Application | Wireshark | Wireshark | 1.2.6 | All | All | All |
| Application | Wireshark | Wireshark | 1.2.7 | All | All | All |
| Application | Wireshark | Wireshark | 1.2.8 | All | All | All |
| Application | Wireshark | Wireshark | 1.2.9 | All | All | All |
| Application | Wireshark | Wireshark | 1.2.2 | All | All | All |
| Application | Wireshark | Wireshark | 1.2.3 | All | All | All |
| Application | Wireshark | Wireshark | 1.2.4 | All | All | All |
| Application | Wireshark | Wireshark | 1.2.5 | All | All | All |
| Application | Wireshark | Wireshark | 1.2.6 | All | All | All |
| Application | Wireshark | Wireshark | 1.2.7 | All | All | All |
| Application | Wireshark | Wireshark | 1.2.8 | All | All | All |
| Application | Wireshark | Wireshark | 1.2.9 | All | All | All |

cpe:2.3:a:wireshark:wireshark:1.2.2:*:*:*:*:*:*:*:

cpe:2.3:a:wireshark:wireshark:1.2.3:*:*:*:*:*:*:*:

cpe:2.3:a:wireshark:wireshark:1.2.4:*:*:*:*:*:*:*:

cpe:2.3:a:wireshark:wireshark:1.2.5:*:*:*:*:*:*:*:

cpe:2.3:a:wireshark:wireshark:1.2.6:*:*:*:*:*:*:*:

cpe:2.3:a:wireshark:wireshark:1.2.7:*:*:*:*:*:*:*

cpe:2.3:a:wireshark:wireshark:1.2.8:*:*:*:*:*:*:*

cpe:2.3:a:wireshark:wireshark:1.2.9:*:*:*:*:*:*:*

cpe:2.3:a:wireshark:wireshark:1.2.2:*:*:*:*:*:*:*

cpe:2.3:a:wireshark:wireshark:1.2.3:*:*:*:*:*:*:*

cpe:2.3:a:wireshark:wireshark:1.2.4:*:*:*:*:*:*:*

cpe:2.3:a:wireshark:wireshark:1.2.5:*:*:*:*:*:*:*

cpe:2.3:a:wireshark:wireshark:1.2.6:*:*:*:*:*:*:*

cpe:2.3:a:wireshark:wireshark:1.2.7:*:*:*:*:*:*:*

cpe:2.3:a:wireshark:wireshark:1.2.8:*:*:*:*:*:*:*

cpe:2.3:a:wireshark:wireshark:1.2.9:*:*:*:*:*:*:*

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→