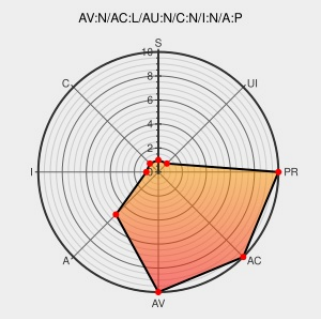
CVE-2013-4931

Published on: 07/29/2013 12:00:00 AM UTC

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

CVE-2013-4931

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



Certain versions of Wireshark from Wireshark contain the following vulnerability:

epan/proto.c in Wireshark 1.8.x before 1.8.9 and 1.10.x before 1.10.1 allows remote attackers to cause a denial of service (loop) via a crafted packet that is not properly handled by the GSM RR dissector.

CVE-2013-4931 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
Red Hat Customer Portal	web.archive.org text/html Inactive Link Not Archived	REDHAT RHSA-2014:0341
openSUSE-SU-2013:1300-1: moderate: wireshark to 1.8.9	lists.opensuse.org text/html	SUSE openSUSE-SU-2013:1300
Security Advisory SA54371 - SUSE update for wireshark - Secunia	web.archive.org text/html	SECUNIA 54371
Wireshark · Wireshark 1.8.9 Release Notes	www.wireshark.org text/html	CONFIRM www.wireshark.org/docs/relnotes/wireshark-1.8.9.html
Repository / Oval Repository	oval.cisecurity.org text/html	OVAL oval:org.mitre.oval:def:17325

8923 – Fuzz failure: very long loop in packet-gsm_a_rr	bugs.wireshark.org text/html	CONFIRM bugs.wireshark.org/bugzilla/show_bug.cgi?id=8923
Security Advisory SA54425 - Gentoo update for wireshark - Secunia	web.archive.org text/html	SECUNIA 54425
code.wireshark Code Review - wireshark.git/tree	Patch anonsvn.wireshark.org text/xml	CONFIRM anonsvn.wireshark.org/viewvc?view=revision&revision=50504
Gentoo Linux Documentation -- Wireshark: Multiple vulnerabilities	www.gentoo.org text/html	GENTOO GLSA-201308-05
Security Advisory SA54296 - Wireshark Multiple Denial of Service Vulnerabilities - Secunia	web.archive.org text/html	SECUNIA 54296
Wireshark · wnpa-sec-2013-49 · GSM RR dissector large loop	Vendor Advisory www.wireshark.org text/html	CONFIRM www.wireshark.org/security/wnpa-sec-2013-49.html
openSUSE-SU-2013:1295-1: moderate: wireshark to 1.8.9	lists.opensuse.org text/html	SUSE openSUSE-SU-2013:1295
Wireshark · Wireshark 1.10.1 Release Notes	www.wireshark.org text/html	CONFIRM www.wireshark.org/docs/relnotes/wireshark-1.10.1.html
code.wireshark Code Review - wireshark.git/tree	Patch anonsvn.wireshark.org text/xml	CONFIRM anonsvn.wireshark.org/viewvc/trunk/epan/proto.c?r1=50504&r2=50503&pathrev=50504

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	1.8.0	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
Application	Wireshark	Wireshark	1.8.4	All	All	All
Application	Wireshark	Wireshark	1.8.5	All	All	All
Application	Wireshark	Wireshark	1.8.6	All	All	All
Application	Wireshark	Wireshark	1.8.7	All	All	All
Application	Wireshark	Wireshark	1.8.8	All	All	All
Application	Wireshark	Wireshark	1.10.0	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
Application	Wireshark	Wireshark	1.8.4	All	All	All
Application	Wireshark	Wireshark	1.8.5	All	All	All
Application	Wireshark	Wireshark	1.8.6	All	All	All
Application	Wireshark	Wireshark	1.8.7	All	All	All
Application	Wireshark	Wireshark	1.8.8	All	All	All

cpe:2.3:a:wireshark:wireshark:1.10.0:*:*:*:*:*:*:*:

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:1.8.4:*:*:*:*:*:*:*:

cpe:2.3:a:wireshark:wireshark:1.8.5:*:*:*:*:*:*:*:

cpe:2.3:a:wireshark:wireshark:1.8.6:*:*:*:*:*:*:*:

cpe:2.3:a:wireshark:wireshark:1.8.7:*:*:*:*:*:*:*:

cpe:2.3:a:wireshark:wireshark:1.8.8:*:*:*:*:*:*:*:

cpe:2.3:a:wireshark:wireshark:1.10.0:*:*:*:*:*:*:*:

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:1.8.4:*:*:*:*:*:*:*:

cpe:2.3:a:wireshark:wireshark:1.8.5:*:*:*:*:*:*:*:

cpe:2.3:a:wireshark:wireshark:1.8.6:*:*:*:*:*:*:*:

cpe:2.3:a:wireshark:wireshark:1.8.7:*:*:*:*:*:*:*:

cpe:2.3:a:wireshark:wireshark:1.8.8:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→

CVE.report and Source URL Uptime Status status.cve.report