



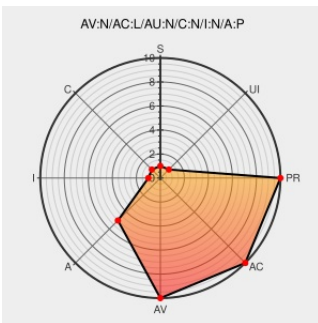
Last Modified on: 03/23/2021 11:28:28 PM UTC

CVE-2013-4079

Source: Mitre

Source: NIST

CVE.ORG

Print: PDF 

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

The `dissect_schedule_message` function in `epan/dissectors/packet-gsm_cbch.c` in the GSM CBCH dissector in Wireshark 1.8.x before 1.8.8 allows remote attackers to cause a denial of service (infinite loop and application hang) via a crafted packet.

CVE-2013-4079 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
Security Advisory SA53762 - Wireshark Multiple Vulnerabilities - Secunia	web.archive.org text/html	 SECUNIA 53762
8730 – GSM_CBCH dissector hangs	Vendor Advisory bugs.wireshark.org text/html	 CONFIRM bugs.wireshark.org/bugzilla/show_bug.cgi?id=8730
Repository / Oval Repository	oval.cisecurity.org text/html	 OVAL oval:org.mitre.oval:def:16691
openSUSE-SU-2013:1086-1: moderate: wireshark	lists.opensuse.org text/html	 SUSE openSUSE-SU-2013:1086
Security Advisory SA54425 - Gentoo update for wireshark - Secunia	web.archive.org text/html	 SECUNIA 54425
openSUSE-SU-2013:1084-1: moderate:	lists.opensuse.org	 SUSE openSUSE-SU-2013:1084

update for wireshark	text/html	
code.wireshark Code Review - wireshark.git/tree	anonsvn.wireshark.org text/xml	 CONFIRM anonsvn.wireshark.org/viewvc/trunk/epan/dissectors/packet-gsm_cbch.c?r1=49686&r2=49685&pathrev=49686
Wireshark · wnpa-sec-2013-37 · GSM CBCB dissector crash	www.wireshark.org text/html	 CONFIRM www.wireshark.org/security/wnpa-sec-2013-37.html
Gentoo Linux Documentation -- Wireshark: Multiple vulnerabilities	www.gentoo.org text/html	 GENTOO GLSA-201308-05
Wireshark · Wireshark 1.8.8 Release Notes	www.wireshark.org text/html	 CONFIRM www.wireshark.org/docs/relnotes/wireshark-1.8.8.html
code.wireshark Code Review - wireshark.git/tree	anonsvn.wireshark.org text/xml	 CONFIRM anonsvn.wireshark.org/viewvc?view=revision&revision=49686

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.

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Opensuse	Opensuse	11.4	All	All	All
Operating System	Opensuse	Opensuse	12.2	All	All	All
Operating System	Opensuse	Opensuse	12.3	All	All	All
Operating System	Opensuse	Opensuse	11.4	All	All	All
Operating System	Opensuse	Opensuse	12.2	All	All	All
Operating System	Opensuse	Opensuse	12.3	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	1.8.0	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
cpe:2.3:o:opensuse:opensuse:11.4:*****:.*:						
cpe:2.3:o:opensuse:opensuse:12.2:*****:.*:						
cpe:2.3:o:opensuse:opensuse:12.3:*****:.*:						
cpe:2.3:o:opensuse:opensuse:11.4:*****:.*:						
cpe:2.3:o:opensuse:opensuse:12.2:*****:.*:						
cpe:2.3:o:opensuse:opensuse:12.3:*****:.*:						
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:1.8.0:*****:.*:						
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:*****:.*:						

NO vendor comments have been submitted for this CVE

[← Previous ID](#)

[Next ID→](#)

© [CVE.report](#) 2023   |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

CVE.report and Source URL Uptime Status [status.cve.report](#)