



CVE-2011-0444

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF](#)

Summary

CVE	CVE-2011-0444
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2011-01-13 01:00:00 UTC
Updated	2017-09-19 01:31:00 UTC
Description	Buffer overflow in the MAC-LTE dissector (epan/dissectors/packet-mac-lte.c) in Wireshark 1.2.0 through 1.2.13 and 1.4.0 tr

Risk And Classification

Problem Types: CWE-119

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Wireshark	Wireshark	1.2	All	All	All
Application	Wireshark	Wireshark	1.2.0	All	All	All
Application	Wireshark	Wireshark	1.2.1	All	All	All
Application	Wireshark	Wireshark	1.2.10	All	All	All
Application	Wireshark	Wireshark	1.2.11	All	All	All
Application	Wireshark	Wireshark	1.2.12	All	All	All
Application	Wireshark	Wireshark	1.2.13	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
Application	Wireshark	Wireshark	1.4.0	All	All	All
Application	Wireshark	Wireshark	1.4.1	All	All	All

Application	Wireshark	Wireshark	1.4.2	All	All	All
Application	Wireshark	Wireshark	1.2	All	All	All
Application	Wireshark	Wireshark	1.2.0	All	All	All
Application	Wireshark	Wireshark	1.2.1	All	All	All
Application	Wireshark	Wireshark	1.2.10	All	All	All
Application	Wireshark	Wireshark	1.2.11	All	All	All
Application	Wireshark	Wireshark	1.2.12	All	All	All
Application	Wireshark	Wireshark	1.2.13	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
Application	Wireshark	Wireshark	1.4.0	All	All	All
Application	Wireshark	Wireshark	1.4.1	All	All	All
Application	Wireshark	Wireshark	1.4.2	All	All	All

References						
Reference			Source	Link	Tags	
Fedora update for wireshark - Secunia.com			SECUNIA	secunia.com		
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH			VUPEN	www.vupen.com	Vendor Ac	
70403			OSVDB	osvdb.org		
Wireshark Dissectors Multiple Vulnerabilities			BID	www.securityfocus.com		
[SECURITY] Fedora 14 Update: wireshark-1.4.3-1.fc14			FEDORA	lists.fedoraproject.org		
Repository / Oval Repository			OVAL	oval.cisecurity.org		
IBM X-Force Exchange			XF	exchange.xforce.ibmcloud.com		
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH			VUPEN	www.vupen.com		
5530 – Buffer overflows in MAC-LTE dissector and SNMP EngineID preferences			CONFIRM	bugs.wireshark.org	Patch	
Wireshark · wnpa-sec-2011-01			CONFIRM	www.wireshark.org		
Wireshark · wnpa-sec-2011-02			CONFIRM	www.wireshark.org		
Support / Security / Advisories // MDVSA-2011:007 Mandriva			MANDRIVA	www.mandriva.com		
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH			VUPEN	www.vupen.com		
[SECURITY] Fedora 14 Update: wireshark-1.4.3-1.fc14			FEDORA	lists.fedoraproject.org		

[SECURITY] Fedora 13 Update: wireshark-1.2.14-1.fc13	FEDORA	lists.fedoraproject.org	
bugs.wireshark.org/bugzilla/attachment.cgi	MISC	bugs.wireshark.org	Patch
Support	REDHAT	www.redhat.com	
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH	VUPEN	www.vupen.com	
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical,

No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.

© [CVE.report](https://cve.report) 2026 |

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](https://mitre.org) and the authoritative source of CVE content is [MITRE's CVE web site](https://mitre.org/cve). This site includes MITRE data granted under the following [license](https://mitre.org/cve).

Free CVE JSON API cve.report/api

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