



CVE-2009-3241

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

Summary

CVE	CVE-2009-3241
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2009-09-18 10:30:00 UTC
Updated	2017-09-19 01:29:00 UTC
Description	Unspecified vulnerability in the OpcUa (OPC UA) dissector in Wireshark 0.99.6 through 1.0.8 and 1.2.0 through 1.2.1 allows

Risk And Classification

Problem Types: NVD-CWE-noinfo

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Wireshark	Wireshark	0.99.6	All	All	All
Application	Wireshark	Wireshark	0.99.6a	All	All	All
Application	Wireshark	Wireshark	0.99.7	All	All	All
Application	Wireshark	Wireshark	0.99.8	All	All	All
Application	Wireshark	Wireshark	0.99.9	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	1.0.5	All	All	All
Application	Wireshark	Wireshark	1.0.6	All	All	All
Application	Wireshark	Wireshark	1.0.7	All	All	All
Application	Wireshark	Wireshark	1.0.8	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	0.99.6	All	All	All
Application	Wireshark	Wireshark	0.99.6a	All	All	All
Application	Wireshark	Wireshark	0.99.7	All	All	All
Application	Wireshark	Wireshark	0.99.8	All	All	All
Application	Wireshark	Wireshark	0.99.9	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	1.0.5	All	All	All
Application	Wireshark	Wireshark	1.0.6	All	All	All
Application	Wireshark	Wireshark	1.0.7	All	All	All
Application	Wireshark	Wireshark	1.0.8	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

References						
Reference			Source	Link	Tags	
Repository / Oval Repository			OVAL	oval.cisecurity.org		
[security-announce] SUSE Security Summary Report: SUSE-SR:2009:016			SUSE	lists.opensuse.org		
Wireshark: Wireshark 1.2.2 Release Notes			CONFIRM	www.wireshark.org		
3986 – some malformed OPC UA traffic causes wireshark to "freeze"			MISC	bugs.wireshark.org		
Security Alerts - Secunia			SECUNIA	secunia.com		
Wireshark: wnpa-sec-2009-05			CONFIRM	www.wireshark.org	Patch, V	
Debian update for wireshark - Secunia Advisories - Vulnerability Information - Secunia.com			SECUNIA	secunia.com		
Wireshark Multiple Denial of Service Vulnerabilities - Secunia.com			SECUNIA	secunia.com	Vendor A	
Wireshark: wnpa-sec-2009-06			CONFIRM	www.wireshark.org	Vendor A	
Debian -- Security Information -- DSA-1942-1 wireshark			DEBIAN	www.debian.org		
Wireshark 1.2.1 Multiple Vulnerabilities			BID	www.securityfocus.com	Exploit	
Wireshark: Wireshark 1.0.9 Release Notes			CONFIRM	www.wireshark.org		
CVE Program record			CVE.ORG	www.cve.org	canonical	

NVD vulnerability detailNVDnvd.nist.govcanonical

Vendor Comments And Credit

Organization	Published	Contributor	Statement
Red Hat	2009-09-30	Tomas Hoger	Not vulnerable. This issue did not affect the versions of wireshark as shipped with Red Hat Enterprise Linux 5.4.

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

© [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](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

Free CVE JSON API [cve.report/api](#)

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