



CVE-2010-4300

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

Summary

CVE	CVE-2010-4300
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2010-11-26 19:00:00 UTC
Updated	2017-09-19 01:31:00 UTC
Description	Heap-based buffer overflow in the dissect_ldss_transfer function (epan/dissectors/packet-ldss.c) in the LDSS dissector in V

Risk And Classification

Problem Types: CWE-119

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Wireshark	Wireshark	1.2.0	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	1.2.2	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	1.2.0	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	1.2.2	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

References						
Reference				Source	Link	
Red Hat update for wireshark - Secunia.com				SECUNIA	secunia.com	
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH				VUPEN	www.vuper	
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH				VUPEN	www.vuper	
Wireshark · wnpa-sec-2010-13				CONFIRM	www.wiresl	
Wireshark LDSS Dissector Buffer Overflow Vulnerability				BID	www.secur	
SecurityTracker.com Archives - Wireshark Buffer Overflow in LDSS Dissector Lets Remote Users Deny Service				SECTRACK	www.secur	
Wireshark LDSS Dissector Buffer Overflow Vulnerability				EXPLOIT-DB	www.exploi	
Support / Security / Advisories / / MDVSA-2010:242 Mandriva				MANDRIVA	www.mand	
Wireshark · wnpa-sec-2010-14				CONFIRM	www.wiresl	
[security-announce] SUSE Security Summary Report: SUSE-SR:2011:001				SUSE	lists.opensu	
Repository / Oval Repository				OVAL	oval.cisecu	
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH				VUPEN	www.vuper	
Wireshark Two Vulnerabilities - Advisories - Community				SECUNIA	secunia.coi	
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH				VUPEN	www.vuper	
Security				CONFIRM	blogs.sun.c	
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH				VUPEN	www.vuper	
Bug 5318 – Buffer Overflow in ldss dissector				CONFIRM	bugs.wiresl	
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH				VUPEN	www.vuper	
SUSE update for multiple packages - Advisories - Community				SECUNIA	secunia.coi	

Support	REDHAT	www.redhat.com
69354	OSVDB	osvdb.org
[security-announce] SUSE Security Summary Report: SUSE-SR:2011:002	SUSE	lists.opensuse.org
SUSE update for Multiple Packages - Secunia.com	SECUNIA	secunia.com
CVE Program record	CVE.ORG	www.cve.org
NVD vulnerability detail	NVD	nvd.nist.gov

No vendor comments have been submitted for this CVE.

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

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

Free CVE JSON API cve.report/api

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