



CVE-2014-7992

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

Summary

CVE	CVE-2014-7992
State	PUBLIC
Assigner	psirt@cisco.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2014-11-18 01:59:00 UTC
Updated	2017-09-08 01:29:00 UTC
Description	The DLSw implementation in Cisco IOS does not initialize packet buffers, which allows remote attackers to obtain sensitive

Risk And Classification

Problem Types: CWE-200

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Cisco	ios	-	All	All	All
Operating System	Cisco	ios	-	All	All	All

References

Reference	Source	Link
Cisco IOS CVE-2014-7992 Information Disclosure Vulnerability	BID	www.securi
20141117 Cisco IOS DLSw Information Disclosure Vulnerability	CISCO	tools.cisco.c
IBM X-Force Exchange	XF	exchange.xl
Cisco IOS DLSw Processing Flaw Lets Remote Users Obtain Potentially Sensitive Information - SecurityTracker	SECTrack	www.securi
tools.cisco.com/security/center/viewAlert.x	CONFIRM	tools.cisco.c
CVE Program record	CVE.ORG	www.cve.or
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](#) 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](#)