



CVE-2014-8714

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

Summary

CVE	CVE-2014-8714
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2014-11-23 02:59:00 UTC
Updated	2023-11-07 02:22:00 UTC
Description	The dissect_write_structured_field function in epan/dissectors/packet-tn5250.c in the TN5250 dissector in Wireshark 1.10.x

Risk And Classification

Problem Types: CWE-399

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Wireshark	Wireshark	1.10.0	All	All	All
Application	Wireshark	Wireshark	1.10.1	All	All	All
Application	Wireshark	Wireshark	1.10.10	All	All	All
Application	Wireshark	Wireshark	1.10.2	All	All	All
Application	Wireshark	Wireshark	1.10.3	All	All	All
Application	Wireshark	Wireshark	1.10.4	All	All	All
Application	Wireshark	Wireshark	1.10.5	All	All	All
Application	Wireshark	Wireshark	1.10.6	All	All	All
Application	Wireshark	Wireshark	1.10.7	All	All	All
Application	Wireshark	Wireshark	1.10.8	All	All	All
Application	Wireshark	Wireshark	1.10.9	All	All	All
Application	Wireshark	Wireshark	1.12.0	All	All	All
Application	Wireshark	Wireshark	1.12.1	All	All	All
Application	Wireshark	Wireshark	1.10.0	All	All	All
Application	Wireshark	Wireshark	1.10.1	All	All	All
Application	Wireshark	Wireshark	1.10.10	All	All	All
Application	Wireshark	Wireshark	1.10.2	All	All	All

Application	Wireshark	Wireshark	1.10.3	All	All	All
Application	Wireshark	Wireshark	1.10.4	All	All	All
Application	Wireshark	Wireshark	1.10.5	All	All	All
Application	Wireshark	Wireshark	1.10.6	All	All	All
Application	Wireshark	Wireshark	1.10.7	All	All	All
Application	Wireshark	Wireshark	1.10.8	All	All	All
Application	Wireshark	Wireshark	1.10.9	All	All	All
Application	Wireshark	Wireshark	1.12.0	All	All	All
Application	Wireshark	Wireshark	1.12.1	All	All	All

References						
Reference	Source		Link	Tags		
Oracle Bulletin Board Update - January 2015	CONFIRM		www.oracle.com			
code.wireshark Code Review - wireshark.git/commit	CONFIRM		code.wireshark.org			
code.wireshark Code Review - wireshark.git/commit			code.wireshark.org			
Wireshark TN5250 Dissector CVE-2014-8714 Infinite Loop Denial of Service Vulnerability	BID		www.securityfocus.com			
code.wireshark Code Review - wireshark.git/commit			code.wireshark.org			
openSUSE-SU-2014:1503-1: moderate: update for wireshark	SUSE		lists.opensuse.org			
Red Hat Customer Portal	REDHAT		rhn.redhat.com			
Wireshark · wnpa-sec-2014-23 · TN5250 infinite loops	CONFIRM		www.wireshark.org	Vendor Ac		
[SECURITY] Fedora 21 Update: wireshark-1.12.2-1.fc21	FEDORA		lists.fedoraproject.org			
Bug 10596 – Buildbot crash output: fuzz-2014-10-19-16935.pcap	CONFIRM		bugs.wireshark.org			
code.wireshark Code Review - wireshark.git/commit	CONFIRM		code.wireshark.org			
Oracle Linux Bulletin - October 2015	CONFIRM		www.oracle.com			
About Secunia Research Flexera	SECUNIA		secunia.com			
Oracle Critical Patch Update - October 2017	CONFIRM		www.oracle.com			
About Secunia Research Flexera	SECUNIA		secunia.com			
Debian -- Security Information -- DSA-3076-1 wireshark	DEBIAN		www.debian.org			
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](#) 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](#)