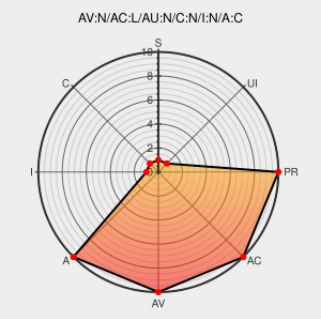
CVE-2013-2487

Published on: 03/07/2013 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:28:42 PM UTC

CVE-2013-2487

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF



Certain versions of Debian Linux from Debian contain the following vulnerability:

epan/dissectors/packet-reload.c in the REsource LOcation And Discovery (aka RELOAD) dissector in Wireshark 1.8.x before 1.8.6 uses incorrect integer data types, which allows remote attackers to cause a denial of service (infinite loop) via crafted integer values in a packet, related to the (1) dissect_icecandidates, (2) dissect_kinddata, (3) dissect_nodeid_list, (4) dissect_storeans, (5) dissect_storereq, (6) dissect_storeddataspecifier, (7) dissect_fetchreq, (8) dissect_findans, (9) dissect_diagnosticinfo, (10) dissect_diagnosticresponse, (11) dissect_reload_messagecontents, and (12) dissect_reload_message functions, a different vulnerability than CVE-2013-2486.

CVE-2013-2487 has been assigned by cve@mitre.org to track the vulnerability

CVSS2 Score: 7.8 - HIGH

Access Vector	Access Complexity	Authentication
NETWORK	LOW	NONE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
NONE	NONE	COMPLETE

CVE References

Description	Tags	Link
Bug 8364 – Denial of Service in packet-reload.c	bugs.wireshark.org text/html	CONFIRM bugs.wireshark.org/bugzilla/show_bug.cgi?id=8364
Security Advisory SA52471 - Wireshark Multiple Denial of Service Vulnerabilities - Secunia	web.archive.org text/html	SECUNIA 52471
openSUSE-SU-2013:0494-1: moderate: wireshark: update to 1.8.6	lists.opensuse.org	SUSE openSUSE-SU-2013:0494

update to 1.8.6	text/html	
openSUSE-SU-2013:0911-1: moderate: update for wireshark	lists.opensuse.org text/html	SUSE openSUSE-SU-2013:0911
openSUSE-SU-2013:0947-1: moderate: update for wireshark	lists.opensuse.org text/html	SUSE openSUSE-SU-2013:0947
Security Advisory SA53425 - Wireshark Multiple Denial of Service Vulnerabilities - Secunia	web.archive.org text/html	SECUNIA 53425
code.wireshark Code Review - wireshark.git/tree	anonsvn.wireshark.org text/xml	CONFIRM anonsvn.wireshark.org/viewvc?view=revision&revision=47808
Wireshark · wnpa-sec-2013-21 · RELOAD dissector infinite loop	Vendor Advisory www.wireshark.org text/html	CONFIRM www.wireshark.org/security/wnpa-sec-2013-21.html
code.wireshark Code Review - wireshark.git/tree	anonsvn.wireshark.org text/xml	CONFIRM anonsvn.wireshark.org/viewvc/trunk/epan/dissectors/packet-reload.c?r1=47808&r2=47807&pathrev=47808
openSUSE-SU-2013:0506-1: moderate: wireshark: update to 1.8.6	lists.opensuse.org text/html	SUSE openSUSE-SU-2013:0506
Wireshark · Wireshark 1.8.6 Release Notes	www.wireshark.org text/html	CONFIRM www.wireshark.org/docs/relnotes/wireshark-1.8.6.html
Repository / Oval Repository	oval.cisecurity.org text/html	OVAL oval:org.mitre.oval:def:16593

By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to comment@cve.report.

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Debian	Debian Linux	7.0	All	All	All
Operating System	Debian	Debian Linux	7.0	All	All	All
Operating System	Opensuse	Opensuse	11.4	All	All	All
Operating System	Opensuse	Opensuse	12.1	All	All	All
Operating System	Opensuse	Opensuse	12.2	All	All	All
Operating System	Opensuse	Opensuse	12.3	All	All	All
Operating System	Opensuse	Opensuse	11.4	All	All	All
Operating System	Opensuse	Opensuse	12.1	All	All	All

Operating System	Opensuse	Opensuse	12.2	All	All	All
Operating System	Opensuse	Opensuse	12.3	All	All	All
Application	Wireshark	Wireshark	1.8.0	All	All	All
Application	Wireshark	Wireshark	1.8.1	All	All	All
Application	Wireshark	Wireshark	1.8.2	All	All	All
Application	Wireshark	Wireshark	1.8.3	All	All	All
Application	Wireshark	Wireshark	1.8.4	All	All	All
Application	Wireshark	Wireshark	1.8.5	All	All	All
Application	Wireshark	Wireshark	1.8.0	All	All	All
Application	Wireshark	Wireshark	1.8.1	All	All	All
Application	Wireshark	Wireshark	1.8.2	All	All	All
Application	Wireshark	Wireshark	1.8.3	All	All	All
Application	Wireshark	Wireshark	1.8.4	All	All	All
Application	Wireshark	Wireshark	1.8.5	All	All	All

cpe:2.3:o:debian:debian_linux:7.0:*:*:*:*:*:*:*

cpe:2.3:o:debian:debian_linux:7.0:*:*:*:*:*:*:*

cpe:2.3:o:opensuse:opensuse:11.4:*:*:*:*:*:*:*

cpe:2.3:o:opensuse:opensuse:12.1:*:*:*:*:*:*:*

cpe:2.3:o:opensuse:opensuse:12.2:*:*:*:*:*:*:*

cpe:2.3:o:opensuse:opensuse:12.3:*:*:*:*:*:*:*

cpe:2.3:o:opensuse:opensuse:11.4:*:*:*:*:*:*:*

cpe:2.3:o:opensuse:opensuse:12.1:*:*:*:*:*:*:*

cpe:2.3:o:opensuse:opensuse:12.2:*:*:*:*:*:*:*

cpe:2.3:o:opensuse:opensuse:12.3:*:*:*:*:*:*:*

cpe:2.3:a:wireshark:wireshark:1.8.0:*:*:*:*:*:*:*

cpe:2.3:a:wireshark:wireshark:1.8.1:*:*:*:*:*:*:*

cpe:2.3:a:wireshark:wireshark:1.8.2:*:*:*:*:*:*:*

cpe:2.3:a:wireshark:wireshark:1.8.3:*:*:*:*:*:*:*

cpe:2.3:a:wireshark:wireshark:1.8.4:*:*:*:*:*:*:*

cpe:2.3:a:wireshark:wireshark:1.8.5:*:*:*:*:*:*:*

cpe:2.3:a:wireshark:wireshark:1.8.0:*:*:*:*:*:*:*

cpe:2.3:a:wireshark:wireshark:1.8.1:*:*:*:*:*:*:*

cpe:2.3:a:wireshark:wireshark:1.8.2:*:*:*:*:*:*:*

cpe:2.3:a:wireshark:wireshark:1.8.3:*:*:*:*:*:*:*

cpe:2.3:a:wireshark:wireshark:1.8.4:*:*:*:*:*:*:*

cpe:2.3:a:wireshark:wireshark:1.8.5:*:*:*:*:*:*:*

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→

© CVE.report 2023 | |
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 registred 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.

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