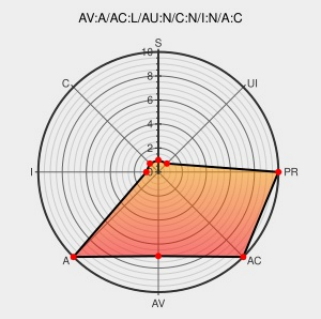
CVE-2013-2486

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

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

CVE-2013-2486

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



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

The dissect_diagnosticrequest function in epan/dissectors/packet-reload.c in the REsource LOcation And Discovery (aka RELOAD) dissector in Wireshark 1.8.x before 1.8.6 uses an incorrect integer data type, which allows remote attackers to cause a denial of service (infinite loop) via crafted integer values in a packet.

CVE-2013-2486 has been assigned by cve@mitre.org to track the vulnerability

CVSS2 Score: 6.1 - MEDIUM

Access Vector	Access Complexity	Authentication
ADJACENT_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 text/html	SUSE openSUSE-SU-2013:0494
Repository / Oval Repository	oval.cisecurity.org text/html	OVAL oval:org.mitre.oval:def:16109
openSUSE-SU-2013:0911-1: moderate: update for wireshark	lists.opensuse.org text/html	SUSE openSUSE-SU-2013:0911
code.wireshark Code Review - wireshark.git/tree		CONFIRM

code.wireshark Code Review - wireshark.git/tree	anonsvn.wireshark.org text/xml	CONFIRM anonsvn.wireshark.org/viewvc/trunk/epan/dissectors/packet-reload.c?r1=47805&r2=47804&pathrev=47805
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=47805
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
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	Vendor Advisory www.wireshark.org text/html	CONFIRM www.wireshark.org/docs/relnotes/wireshark-1.8.6.html

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→