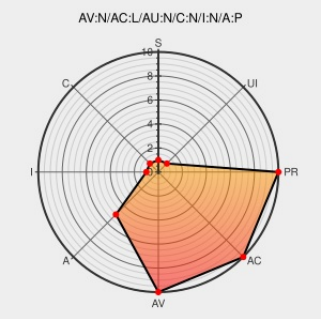
CVE-2013-7114

Published on: 12/19/2013 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:28:34 PM UTC

CVE-2013-7114

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



Certain versions of Wireshark from Wireshark contain the following vulnerability:

Multiple buffer overflows in the create_ntlmssp_v2_key function in epan/dissectors/packet-ntlmssp.c in the NTLMSSP v2 dissector in Wireshark 1.8.x before 1.8.12 and 1.10.x before 1.10.4 allow remote attackers to cause a denial of service (application crash) via a long domain name in a packet.

CVE-2013-7114 has been assigned by cve@mitre.org to track the vulnerability

CVSS2 Score: 5 - MEDIUM

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

CVE References

Description	Tags	Link
Support / Security / Advisories / / MDVSA-2013:296 | Mandriva	www.mandriva.com text/html	MANDRIVA MDVSA-2013:296
code.wireshark Code Review - wireshark.git/tree	Patch anonsvn.wireshark.org text/xml	CONFIRM anonsvn.wireshark.org/viewvc/trunk/epan/dissectors/packet-ntlmssp.c?r1=53626&r2=53625&pathrev=53626
openSUSE-SU-2014:0020-1: moderate: update for wireshark	lists.opensuse.org text/html	SUSE openSUSE-SU-2014:0020
Security Advisory SA56313 - SUSE update for wireshark - Secunia	web.archive.org text/html	SECUNIA 56313
Security Advisory SA56052 - Debian update for wireshark - Secunia	web.archive.org text/html	SECUNIA 56052

openSUSE-SU-2014:0017-1: moderate: update for wireshark	lists.opensuse.org text/html	SUSE openSUSE-SU-2014:0017
Wireshark · wnpa-sec-2013-68 · NTLMSSP v2 dissector crash	Vendor Advisory www.wireshark.org text/html	CONFIRM www.wireshark.org/security/wnpa-sec-2013-68.html
Security Advisory SA56285 - SUSE update for wireshark - Secunia	web.archive.org text/html	SECUNIA 56285
openSUSE-SU-2014:0013-1: moderate: update for wireshark	lists.opensuse.org text/html	SUSE openSUSE-SU-2014:0013
Debian -- Security Information -- DSA-2825-1 wireshark	www.debian.org Depreciated Link text/html	DEBIAN DSA-2825
code.wireshark Code Review - wireshark.git/tree	Patch anonsvn.wireshark.org text/xml	CONFIRM anonsvn.wireshark.org/viewvc?view=revision&revision=53626
Red Hat Customer Portal	web.archive.org text/html Inactive Link Not Archived	REDHAT RHSA-2014:0342

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

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	1.10.2	All	All	All
Application	Wireshark	Wireshark	1.10.3	All	All	All
Application	Wireshark	Wireshark	1.8.0	All	All	All
Application	Wireshark	Wireshark	1.8.1	All	All	All
Application	Wireshark	Wireshark	1.8.10	All	All	All
Application	Wireshark	Wireshark	1.8.11	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	1.8.6	All	All	All
Application	Wireshark	Wireshark	1.8.7	All	All	All
Application	Wireshark	Wireshark	1.8.8	All	All	All

Application	Wireshark	Wireshark	1.8.9	All	All	All
Application	Wireshark	Wireshark	1.10.0	All	All	All
Application	Wireshark	Wireshark	1.10.1	All	All	All
Application	Wireshark	Wireshark	1.10.2	All	All	All
Application	Wireshark	Wireshark	1.10.3	All	All	All
Application	Wireshark	Wireshark	1.8.0	All	All	All
Application	Wireshark	Wireshark	1.8.1	All	All	All
Application	Wireshark	Wireshark	1.8.10	All	All	All
Application	Wireshark	Wireshark	1.8.11	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	1.8.6	All	All	All
Application	Wireshark	Wireshark	1.8.7	All	All	All
Application	Wireshark	Wireshark	1.8.8	All	All	All
Application	Wireshark	Wireshark	1.8.9	All	All	All

cpe:2.3:a:wireshark:wireshark:1.10.0:*:*:*:*:*:*:*:

cpe:2.3:a:wireshark:wireshark:1.10.1:*:*:*:*:*:*:*:

cpe:2.3:a:wireshark:wireshark:1.10.2:*:*:*:*:*:*:*:

cpe:2.3:a:wireshark:wireshark:1.10.3:*:*:*:*:*:*:*:

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

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

cpe:2.3:a:wireshark:wireshark:1.8.10:*:*:*:*:*:*:*:

cpe:2.3:a:wireshark:wireshark:1.8.11:*:*:*:*:*:*:*:

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:1.8.6:*:*:*:*:*:*:*:

cpe:2.3:a:wireshark:wireshark:1.8.7:*:*:*:*:*:*:*:

cpe:2.3:a:wireshark:wireshark:1.8.8:*:*:*:*:*:*:*

cpe:2.3:a:wireshark:wireshark:1.8.9:*:*:*:*:*:*:*

cpe:2.3:a:wireshark:wireshark:1.10.0:*:*:*:*:*:*:*

cpe:2.3:a:wireshark:wireshark:1.10.1:*:*:*:*:*:*:*

cpe:2.3:a:wireshark:wireshark:1.10.2:*:*:*:*:*:*:*

cpe:2.3:a:wireshark:wireshark:1.10.3:*:*:*:*:*:*:*

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

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

cpe:2.3:a:wireshark:wireshark:1.8.10:*:*:*:*:*:*:*

cpe:2.3:a:wireshark:wireshark:1.8.11:*:*:*:*:*:*:*

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:1.8.6:*:*:*:*:*:*:*

cpe:2.3:a:wireshark:wireshark:1.8.7:*:*:*:*:*:*:*

cpe:2.3:a:wireshark:wireshark:1.8.8:*:*:*:*:*:*:*

cpe:2.3:a:wireshark:wireshark:1.8.9:*:*:*:*:*:*:*

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→