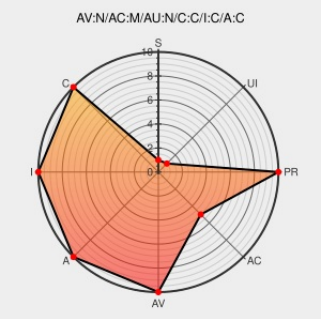
CVE-2011-3360

Published on: 09/20/2011 12:00:00 AM UTC

Last Modified on: 02/13/2023 04:13:19 AM UTC

CVE-2011-3360

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



Certain versions of Wireshark from Wireshark contain the following vulnerability:

Untrusted search path vulnerability in Wireshark 1.4.x before 1.4.9 and 1.6.x before 1.6.2 allows local users to gain privileges via a Trojan horse Lua script in an unspecified directory.

CVE-2011-3360 has been assigned by secalert@redhat.com to track the vulnerability

CVSS2 Score: 9.3 - HIGH

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

CVE References

Description	Tags	Link
oss-security - Re: CVE Request: Multiple issues fixed in wireshark 1.6.2	www.openwall.com text/html	MLIST [oss-security] 20110914 Re: CVE Request: Multiple issues fixed in wireshark 1.6.2
Support / Security / Advisories / / MDVSA-2011:138 | Mandriva	www.mandriva.com text/html	MANDRIVA MDVSA-2011:138
Debian -- Security Information -- DSA-2324-1 wireshark	www.debian.org Depreciated Link text/html	DEBIAN DSA-2324
Repository / Oval Repository	oval.cisecurity.org text/html	OVAL oval:org.mitre.oval:def:15059
No Description Provided	osvdb.org Inactive Link Not Archived	OSVDB 75347

Wireshark · wnpa-sec-2011-15	Vendor Advisory www.wireshark.org text/html	CONFIRM www.wireshark.org/security/wnpa-sec-2011-15.html
Bug 737784 – CVE-2011-3360 Wireshark: Lua script execution vulnerability	bugzilla.redhat.com text/html	CONFIRM bugzilla.redhat.com/show_bug.cgi?id=737784
6136 – [MSVR-11-0078] - Wireshark Arbitrary Script Execution VUlnerability	bugs.wireshark.org text/html	CONFIRM bugs.wireshark.org/bugzilla/show_bug.cgi?id=6136
oss-security - CVE Request: Multiple issues fixed in wireshark 1.6.2	www.openwall.com text/html	MLIST [oss-security] 20110913 CVE Request: Multiple issues fixed in wireshark 1.6.2

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	1.4.0	All	All	All
Application	Wireshark	Wireshark	1.4.1	All	All	All
Application	Wireshark	Wireshark	1.4.2	All	All	All
Application	Wireshark	Wireshark	1.4.3	All	All	All
Application	Wireshark	Wireshark	1.4.4	All	All	All
Application	Wireshark	Wireshark	1.4.5	All	All	All
Application	Wireshark	Wireshark	1.4.6	All	All	All
Application	Wireshark	Wireshark	1.4.7	All	All	All
Application	Wireshark	Wireshark	1.4.8	All	All	All
Application	Wireshark	Wireshark	1.6.0	All	All	All
Application	Wireshark	Wireshark	1.6.1	All	All	All
Application	Wireshark	Wireshark	1.4.0	All	All	All
Application	Wireshark	Wireshark	1.4.1	All	All	All
Application	Wireshark	Wireshark	1.4.2	All	All	All
Application	Wireshark	Wireshark	1.4.3	All	All	All
Application	Wireshark	Wireshark	1.4.4	All	All	All
Application	Wireshark	Wireshark	1.4.5	All	All	All
Application	Wireshark	Wireshark	1.4.6	All	All	All
Application	Wireshark	Wireshark	1.4.7	All	All	All
Application	Wireshark	Wireshark	1.4.8	All	All	All
Application	Wireshark	Wireshark	1.6.0	All	All	All

Application	Wireshark	Wireshark	1.6.1	All	All	All

cpe:2.3:a:wireshark:wireshark:1.4.0:*:*:*:*:*:*:*
cpe:2.3:a:wireshark:wireshark:1.4.1:*:*:*:*:*:*:*
cpe:2.3:a:wireshark:wireshark:1.4.2:*:*:*:*:*:*:*
cpe:2.3:a:wireshark:wireshark:1.4.3:*:*:*:*:*:*:*
cpe:2.3:a:wireshark:wireshark:1.4.4:*:*:*:*:*:*:*
cpe:2.3:a:wireshark:wireshark:1.4.5:*:*:*:*:*:*:*
cpe:2.3:a:wireshark:wireshark:1.4.6:*:*:*:*:*:*:*
cpe:2.3:a:wireshark:wireshark:1.4.7:*:*:*:*:*:*:*
cpe:2.3:a:wireshark:wireshark:1.4.8:*:*:*:*:*:*:*
cpe:2.3:a:wireshark:wireshark:1.6.0:*:*:*:*:*:*:*
cpe:2.3:a:wireshark:wireshark:1.6.1:*:*:*:*:*:*:*
cpe:2.3:a:wireshark:wireshark:1.4.0:*:*:*:*:*:*:*
cpe:2.3:a:wireshark:wireshark:1.4.1:*:*:*:*:*:*:*
cpe:2.3:a:wireshark:wireshark:1.4.2:*:*:*:*:*:*:*
cpe:2.3:a:wireshark:wireshark:1.4.3:*:*:*:*:*:*:*
cpe:2.3:a:wireshark:wireshark:1.4.4:*:*:*:*:*:*:*
cpe:2.3:a:wireshark:wireshark:1.4.5:*:*:*:*:*:*:*
cpe:2.3:a:wireshark:wireshark:1.4.6:*:*:*:*:*:*:*
cpe:2.3:a:wireshark:wireshark:1.4.7:*:*:*:*:*:*:*
cpe:2.3:a:wireshark:wireshark:1.4.8:*:*:*:*:*:*:*
cpe:2.3:a:wireshark:wireshark:1.6.0:*:*:*:*:*:*:*
cpe:2.3:a:wireshark:wireshark:1.6.1:*:*:*:*:*:*:*

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→

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