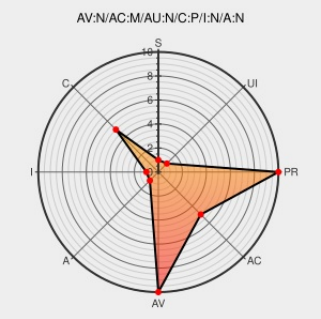
CVE-2011-2192

Published on: 07/07/2011 12:00:00 AM UTC

Last Modified on: 02/13/2023 01:09:22 AM UTC

CVE-2011-2192

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



Certain versions of Mac Os X from Apple contain the following vulnerability:

The Curl_input_negotiate function in http_negotiate.c in libcurl 7.10.6 through 7.21.6, as used in curl and other products, always performs credential delegation during GSSAPI authentication, which allows remote servers to impersonate clients via GSSAPI requests.

CVE-2011-2192 has been assigned by secalert@redhat.com to track the vulnerability

CVSS2 Score: 4.3 - MEDIUM

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

CVE References

Description	Tags	Link
APPLE-SA-2012-02-01-1 OS X Lion v10.7.3 and Security Update 2012-001	Mailing List, Third Party Advisory, lists.apple.com, text/html	APPLE APPLE-SA-2012-02-01-1
Support / Security / Advisories / / MDVSA-2011:116 | Mandriva	Third Party Advisory, www.mandriva.com, text/html	MANDRIVA MDVSA-2011:116
[SECURITY] Fedora 14 Update: curl-7.21.0-8.fc14	Mailing List, Third Party Advisory, lists.fedoraproject.org, text/html	FEDORA FEDORA-2011-8640
711454 – (CVE-2011-2192) CVE-2011-2192 curl: Improper delegation of client credentials during GSS negotiation	Issue Tracking, Third Party Advisory, bugzilla.redhat.com	CONFIRM bugzilla.redhat.com/show_bug.cgi?id=711454

	text/html	
cURL GSS/Negotiate Mechanism Discloses Credentials to Remote Servers - SecurityTracker	Third Party Advisory VDB Entry www.securitytracker.com text/html	SECTRACK 1025713
Gentoo Linux Documentation -- cURL: Multiple vulnerabilities	Third Party Advisory security.gentoo.org text/html	GENTOO GLSA-201203-02
USN-1158-1: curl vulnerabilities | Ubuntu	Third Party Advisory www.ubuntu.com text/html	UBUNTU USN-1158-1
Security Advisory SA48256 - Gentoo update for curl - Secunia	Third Party Advisory web.archive.org text/html	SECUNIA 48256
Debian -- Security Information -- DSA-2271-1 curl	Third Party Advisory www.debian.org Depreciated Link text/html	DEBIAN DSA-2271
[SECURITY] Fedora 15 Update: curl-7.21.3-8.fc15	Mailing List Third Party Advisory lists.fedoraproject.org text/html	FEDORA FEDORA-2011-8586
Fedora update for curl - Secunia.com	Third Party Advisory web.archive.org text/html	SECUNIA 45181
curl: page not found	Broken Link curl.haxx.se text/x-diff Inactive Link Not Archived	CONFIRM curl.haxx.se/curl-gssapi-delegation.patch
Debian update for curl - Secunia.com	Third Party Advisory web.archive.org text/html	SECUNIA 45088
Ubuntu update for curl - Secunia.com	Third Party Advisory web.archive.org text/html	SECUNIA 45047
About the security content of OS X Lion v10.7.3 and Security Update 2012-001	Third Party Advisory support.apple.com text/html	CONFIRM support.apple.com/kb/HT5130
Red Hat update for curl - Secunia.com	Third Party Advisory web.archive.org text/html	SECUNIA 45144
cURL GSSAPI Credential Delegation Weakness - Secunia.com	Third Party Advisory web.archive.org text/html	SECUNIA 45067
Support	Third Party Advisory www.redhat.com text/html	REDHAT RHSA-2011:0918
cURL - Security Advisory (June 23, 2011)	Vendor Advisory curl.haxx.se text/html	CONFIRM curl.haxx.se/docs/adv_20110623.html

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	Apple	Mac Os X	All	All	All	All
Operating System	Apple	Mac Os X	All	All	All	All
Operating System	Canonical	Ubuntu Linux	10.04	All	All	All
Operating System	Canonical	Ubuntu Linux	10.10	All	All	All
Operating System	Canonical	Ubuntu Linux	11.04	All	All	All
Operating System	Canonical	Ubuntu Linux	8.04	All	All	All
Operating System	Canonical	Ubuntu Linux	10.04	All	All	All
Operating System	Canonical	Ubuntu Linux	10.10	All	All	All
Operating System	Canonical	Ubuntu Linux	11.04	All	All	All
Operating System	Canonical	Ubuntu Linux	8.04	All	All	All
Operating System	Debian	Debian Linux	5.0	All	All	All
Operating System	Debian	Debian Linux	6.0	All	All	All
Operating System	Debian	Debian Linux	7.0	All	All	All
Operating System	Debian	Debian Linux	5.0	All	All	All
Operating System	Debian	Debian Linux	6.0	All	All	All
Operating System	Debian	Debian Linux	7.0	All	All	All
Operating System	Fedoraproject	Fedora	14	All	All	All
Operating System	Fedoraproject	Fedora	15	All	All	All
Operating	Fedoraproject	Fedora	14	All	All	All

System						
Operating System	Fedoraproject	Fedora	15	All	All	All
Application	Haxx	Libcurl	All	All	All	All

cpe:2.3:o:apple:mac_os_x:*:*:*:*:*:*:*:*:

cpe:2.3:o:apple:mac_os_x:*:*:*:*:*:*:*:*:

cpe:2.3:o:canonical:ubuntu_linux:10.04:*:*:*:lts:*:*:*:

cpe:2.3:o:canonical:ubuntu_linux:10.10:*:*:*:*:*:*:*:

cpe:2.3:o:canonical:ubuntu_linux:11.04:*:*:*:*:*:*:*:

cpe:2.3:o:canonical:ubuntu_linux:8.04:*:*:*:lts:*:*:*:

cpe:2.3:o:canonical:ubuntu_linux:10.04:*:*:*:lts:*:*:*:

cpe:2.3:o:canonical:ubuntu_linux:10.10:*:*:*:*:*:*:*:

cpe:2.3:o:canonical:ubuntu_linux:11.04:*:*:*:*:*:*:*:

cpe:2.3:o:canonical:ubuntu_linux:8.04:*:*:*:lts:*:*:*:

cpe:2.3:o:debian:debian_linux:5.0:*:*:*:*:*:*:*:

cpe:2.3:o:debian:debian_linux:6.0:*:*:*:*:*:*:*:

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

cpe:2.3:o:debian:debian_linux:5.0:*:*:*:*:*:*:*:

cpe:2.3:o:debian:debian_linux:6.0:*:*:*:*:*:*:*:

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

cpe:2.3:o:fedoraproject:fedora:14:*:*:*:*:*:*:*:

cpe:2.3:o:fedoraproject:fedora:15:*:*:*:*:*:*:*:

cpe:2.3:o:fedoraproject:fedora:14:*:*:*:*:*:*:*:

cpe:2.3:o:fedoraproject:fedora:15:*:*:*:*:*:*:*:

cpe:2.3:a:haxx:libcurl:*:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→

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