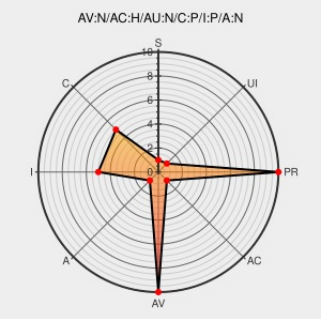
CVE-2013-6422

Published on: 12/23/2013 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:28:37 PM UTC

CVE-2013-6422

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



Certain versions of Ubuntu Linux from Canonical contain the following vulnerability:

The GnuTLS backend in libcurl 7.21.4 through 7.33.0, when disabling digital signature verification (CURLOPT_SSL_VERIFYPEER), also disables the CURLOPT_SSL_VERIFYHOST check for CN or SAN host name fields, which makes it easier for remote attackers to spoof servers and conduct man-in-the-middle (MITM) attacks.

CVE-2013-6422 has been assigned by secalert@redhat.com to track the vulnerability

CVSS2 Score: 4 - MEDIUM

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

CVE References

Description	Tags	Link
cURL - Security Advisory (cert name check ignore GnuTLS)	Vendor Advisory, curl.haxx.se, text/html	CONFIRM curl.haxx.se/docs/adv_20131217.html
Oracle Critical Patch Update - July 2015	www.oracle.com, text/html	CONFIRM www.oracle.com/technetwork/topics/security/cpujul2015-2367936.html
HP Support document - HP Support Center	h20564.www2.hp.com, text/html	HP HPSBMU03112
Debian -- Security Information -- DSA-2824-1 curl	www.debian.org, Depreciated Link, text/html	DEBIAN DSA-2824

USN-2058-1: curl vulnerability | Ubuntu www.ubuntu.com text/html UBUNTU USN-2058-1

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.

Related QID Numbers

670302 EulerOS Security Update for curl (EulerOS-SA-2021-1774)

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Canonical	Ubuntu Linux	12.04	-	lts	All
Operating System	Canonical	Ubuntu Linux	12.10	All	All	All
Operating System	Canonical	Ubuntu Linux	13.04	All	All	All
Operating System	Canonical	Ubuntu Linux	13.10	All	All	All
Operating System	Canonical	Ubuntu Linux	12.04	-	lts	All
Operating System	Canonical	Ubuntu Linux	12.10	All	All	All
Operating System	Canonical	Ubuntu Linux	13.04	All	All	All
Operating System	Canonical	Ubuntu Linux	13.10	All	All	All
Operating System	Debian	Debian Linux	7.0	All	All	All
Operating System	Debian	Debian Linux	7.0	All	All	All
Application	Haxx	Libcurl	7.21.4	All	All	All
Application	Haxx	Libcurl	7.21.5	All	All	All
Application	Haxx	Libcurl	7.21.6	All	All	All
Application	Haxx	Libcurl	7.21.7	All	All	All
Application	Haxx	Libcurl	7.22.0	All	All	All
Application	Haxx	Libcurl	7.23.0	All	All	All
Application	Haxx	Libcurl	7.23.1	All	All	All
Application	Haxx	Libcurl	7.24.0	All	All	All
Application	Haxx	Libcurl	7.25.0	All	All	All
Application	Haxx	Libcurl	7.26.0	All	All	All

Application	Haxx	Libcurl	7.27.0	All	All	All
Application	Haxx	Libcurl	7.28.0	All	All	All
Application	Haxx	Libcurl	7.28.1	All	All	All
Application	Haxx	Libcurl	7.29.0	All	All	All
Application	Haxx	Libcurl	7.30.0	All	All	All
Application	Haxx	Libcurl	7.31.0	All	All	All
Application	Haxx	Libcurl	7.32.0	All	All	All
Application	Haxx	Libcurl	7.33.0	All	All	All
Application	Haxx	Libcurl	7.21.4	All	All	All
Application	Haxx	Libcurl	7.21.5	All	All	All
Application	Haxx	Libcurl	7.21.6	All	All	All
Application	Haxx	Libcurl	7.21.7	All	All	All
Application	Haxx	Libcurl	7.22.0	All	All	All
Application	Haxx	Libcurl	7.23.0	All	All	All
Application	Haxx	Libcurl	7.23.1	All	All	All
Application	Haxx	Libcurl	7.24.0	All	All	All
Application	Haxx	Libcurl	7.25.0	All	All	All
Application	Haxx	Libcurl	7.26.0	All	All	All
Application	Haxx	Libcurl	7.27.0	All	All	All
Application	Haxx	Libcurl	7.28.0	All	All	All
Application	Haxx	Libcurl	7.28.1	All	All	All
Application	Haxx	Libcurl	7.29.0	All	All	All
Application	Haxx	Libcurl	7.30.0	All	All	All
Application	Haxx	Libcurl	7.31.0	All	All	All
Application	Haxx	Libcurl	7.32.0	All	All	All
Application	Haxx	Libcurl	7.33.0	All	All	All

cpe:2.3:o:canonical:ubuntu_linux:12.04:-:lts:*:*:*:*:*:

cpe:2.3:o:canonical:ubuntu_linux:12.10:*:*:*:*:*:*:*:

cpe:2.3:o:canonical:ubuntu_linux:13.04:*:*:*:*:*:*:*:

cpe:2.3:o:canonical:ubuntu_linux:13.10:*:*:*:*:*:*:*:

cpe:2.3:o:canonical:ubuntu_linux:12.04:-:lts:*:*:*:*:*:

cpe:2.3:o:canonical:ubuntu_linux:12.10:*:*:*:*:*:*:*:

cpe:2.3:o:canonical:ubuntu_linux:13.04:*:*:*:*:*:*:*:

cpe:2.3:o:canonical:ubuntu_linux:13.10:*:*:*:*:*:*:*:

cpe:2.3:o:canonical:ubuntu_linux:15.10:*:*:*:*:*:*:*

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

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

cpe:2.3:a:haxx:libcurl:7.21.4:*:*:*:*:*:*:*

cpe:2.3:a:haxx:libcurl:7.21.5:*:*:*:*:*:*:*

cpe:2.3:a:haxx:libcurl:7.21.6:*:*:*:*:*:*:*

cpe:2.3:a:haxx:libcurl:7.21.7:*:*:*:*:*:*:*

cpe:2.3:a:haxx:libcurl:7.22.0:*:*:*:*:*:*:*

cpe:2.3:a:haxx:libcurl:7.23.0:*:*:*:*:*:*:*

cpe:2.3:a:haxx:libcurl:7.23.1:*:*:*:*:*:*:*

cpe:2.3:a:haxx:libcurl:7.24.0:*:*:*:*:*:*:*

cpe:2.3:a:haxx:libcurl:7.25.0:*:*:*:*:*:*:*

cpe:2.3:a:haxx:libcurl:7.26.0:*:*:*:*:*:*:*

cpe:2.3:a:haxx:libcurl:7.27.0:*:*:*:*:*:*:*

cpe:2.3:a:haxx:libcurl:7.28.0:*:*:*:*:*:*:*

cpe:2.3:a:haxx:libcurl:7.28.1:*:*:*:*:*:*:*

cpe:2.3:a:haxx:libcurl:7.29.0:*:*:*:*:*:*:*

cpe:2.3:a:haxx:libcurl:7.30.0:*:*:*:*:*:*:*

cpe:2.3:a:haxx:libcurl:7.31.0:*:*:*:*:*:*:*

cpe:2.3:a:haxx:libcurl:7.32.0:*:*:*:*:*:*:*

cpe:2.3:a:haxx:libcurl:7.33.0:*:*:*:*:*:*:*

cpe:2.3:a:haxx:libcurl:7.21.4:*:*:*:*:*:*:*

cpe:2.3:a:haxx:libcurl:7.21.5:*:*:*:*:*:*:*

cpe:2.3:a:haxx:libcurl:7.21.6:*:*:*:*:*:*:*

cpe:2.3:a:haxx:libcurl:7.21.7:*:*:*:*:*:*:*

cpe:2.3:a:haxx:libcurl:7.22.0:*:*:*:*:*:*:*

cpe:2.3:a:haxx:libcurl:7.23.0:*:*:*:*:*:*:*

cpe:2.3:a:haxx:libcurl:7.23.1:*:*:*:*:*:*:*

cpe:2.3:a:haxx:libcurl:7.24.0:*:*:*:*:*:*:*

cpe:2.3:a:haxx:libcurl:7.25.0:*:*:*:*:*:*:*

cpe:2.3:a:haxx:libcurl:7.26.0:*:*:*:*:*:*:*

cpe:2.3:a:haxx:libcurl:7.27.0:*:*:*:*:*:*:*

cpe:2.3:a:haxx:libcurl:7.28.0:*:*:*:*:*:*:*

cpe:2.3:a:haxx:libcurl:7.28.1:*:*:*:*:*:*:*

cpe:2.3:a:haxx:libcurl:7.29.0:*:*:*:*:*:*:*

cpe:2.3:a:haxx:libcurl:7.30.0:*:*:*:*:*:*:*

cpe:2.3:a:haxx:libcurl:7.31.0:*:*:*:*:*:*:*

cpe:2.3:a:haxx:libcurl:7.32.0:*:*:*:*:*:*:*

cpe:2.3:a:haxx:libcurl:7.33.0:*:*:*:*:*:*:*

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→