

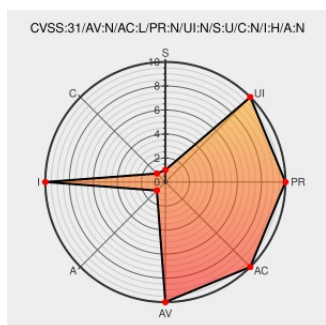


CVE-2012-6071

Published on: 11/19/2019 12:00:00 AM UTC

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

CVE-2012-6071

[Source: Mitre](#)[Source: NIST](#)[CVE.ORG](#)[Print: PDF](#) 

Certain versions of [Debian Linux](#) from [Debian](#) contain the following vulnerability:

nuSOAP before 0.7.3-5 does not properly check the hostname of a cert.

CVE-2012-6071 has been assigned by secalert@redhat.com to track the vulnerability - currently rated as **HIGH** severity.

Affected Vendor/Software: **nussoap** - nussoap version **0.9.5-2**

CVSS3 Score: **7.5 - HIGH**

Attack Vector	Attack Complexity	Privileges Required	User Interaction
NETWORK	LOW	NONE	NONE
Scope	Confidentiality Impact	Integrity Impact	Availability Impact
UNCHANGED	NONE	HIGH	NONE

CVSS2 Score: **5 - MEDIUM**

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

CVE References

Description	Tags	Link
CVE-2012-6071	Third Party Advisory security-tracker.debian.org text/html	MISC security-tracker.debian.org/tracker/CVE-2012-6071

#696707 - nusoap: CVE-2012-6071: wrong CURLOPT_SSL_VERIFYHOST:
do not check hostname of cert - Debian Bug report logs

Issue Tracking
Third Party Advisory
bugs.debian.org
text/html

MISC bugs.debian.org/cgi-bin/bugreport.cgi?bug=696707

oss-security - Re: CVE request: Curl insecure usage

Mailing List
Third Party Advisory
www.openwall.com
text/html

MISC
www.openwall.com/lists/oss-security/2013/01/15/6

oss-security - Re: CVE request: Curl insecure usage

Mailing List
Third Party Advisory
www.openwall.com
text/html

MISC
www.openwall.com/lists/oss-security/2012/12/27/1

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.

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	10.0	All	All	All
Operating System	Debian	Debian Linux	8.0	All	All	All
Operating System	Debian	Debian Linux	9.0	All	All	All
Operating System	Debian	Debian Linux	10.0	All	All	All
Operating System	Debian	Debian Linux	8.0	All	All	All
Operating System	Debian	Debian Linux	9.0	All	All	All
Application	Nusoap Project	Nusoap	All	All	All	All
Application	Nusoap Project	Nusoap	All	All	All	All

cpe:2.3:o:debian:debian_linux:10.0:*:*:*:*:*:

cpe:2.3:o:debian:debian_linux:8.0:*:*:*:*:*:

cpe:2.3:o:debian:debian_linux:9.0:*:*:*:*:*:

cpe:2.3:o:debian:debian_linux:10.0:*:*:*:*:*:

cpe:2.3:o:debian:debian_linux:8.0:*:*:*:*:*:

cpe:2.3:o:debian:debian_linux:9.0:*:*:*:*:*:

cpe:2.3:a:nusoap_project:nusoap:*****:

cpe:2.3:a:nusoap_project:nusoap:*****:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→