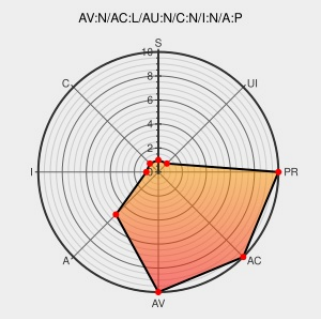
CVE-2011-1473

Published on: 06/16/2012 12:00:00 AM UTC

Last Modified on: 04/20/2021 04:15:00 PM UTC

CVE-2011-1473

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



Certain versions of Openssl from Openssl contain the following vulnerability:

** DISPUTED ** OpenSSL before 0.9.8l, and 0.9.8m through 1.x, does not properly restrict client-initiated renegotiation within the SSL and TLS protocols, which might make it easier for remote attackers to cause a denial of service (CPU consumption) by performing many renegotiations within a single connection, a different vulnerability than CVE-2011-5094. NOTE: it can also be argued that it is the responsibility of server deployments, not a security library, to prevent or limit renegotiation when it is inappropriate within a specific environment.

CVE-2011-1473 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
Pony Mail!	lists.apache.org text/html	MLIST [rocketmq-dev] 20210311 [GitHub] [rocketmq] vongosling merged pull request #1820: [ISSUE #1233] Fix CVE-2011-1473
Re: [TLS] SSL Renegotiation DOS	www.ietf.org text/html	MLIST [tls] 20110315 Re: SSL Renegotiation DOS
Pony Mail!	lists.apache.org text/html	MLIST [rocketmq-commits] 20210311 [rocketmq] branch develop updated: [ISSUE #1233] Fix CVE-2011-1473
Pony Mail!	lists.apache.org text/html	MLIST [rocketmq-dev] 20210420 [GitHub] [rocketmq] mouzz commented on pull request #1820: [ISSUE #1233] Fix CVE-2011-1473

Pony Mail!	lists.apache.org text/html	MLIST [rocketmq-dev] 20191024 [GitHub] [rocketmq] Journey-x commented on issue #1233: TLS Client-initiated renegotiation attack (CVE-2011-1473)
707065 – (CVE-2011-1473) CVE-2011-1473 openssl: DoS via repeated SSL session renegotiations	bugzilla.redhat.com text/html	MISC bugzilla.redhat.com/show_bug.cgi?id=707065
Re: [TLS] SSL Renegotiation DOS	www.ietf.org text/html	MLIST [tls] 20110318 Re: SSL Renegotiation DOS
Re: [TLS] SSL Renegotiation DOS	www.ietf.org text/html	MLIST [tls] 20110318 Re: SSL Renegotiation DOS
Pony Mail!	lists.apache.org text/html	MLIST [rocketmq-dev] 20210420 [GitHub] [rocketmq] mouzz removed a comment on pull request #1820: [ISSUE #1233] Fix CVE-2011-1473
Pony Mail!	lists.apache.org text/html	MLIST [rocketmq-dev] 20210311 [GitHub] [rocketmq] vongosling closed issue #1233: TLS Client-initiated renegotiation attack (CVE-2011-1473)
SSL computational DoS mitigation | Vincent Bernat	vincent.bernat.im text/html	MISC vincent.bernat.im/en/blog/2011-ssl-dos-mitigation.html
[TLS] SSL Renegotiation DOS	www.ietf.org text/html	MLIST [tls] 20110315 SSL Renegotiation DOS
Pony Mail!	lists.apache.org text/html	MLIST [rocketmq-dev] 20200305 [GitHub] [rocketmq] ShadowySpirits opened a new pull request #1820: [ISSUE #1233] Fix CVE-2011-1473
SSL/TLS and Computational DoS - Educated Guesswork	www.educatedguesswork.org text/html	MISC www.educatedguesswork.org/2011/10/ssltls_and_computational_dos.html
Pony Mail!	lists.apache.org text/html	MLIST [rocketmq-dev] 20210327 [GitHub] [rocketmq] liufeiguo commented on pull request #1820: [ISSUE #1233] Fix CVE-2011-1473
Pony Mail!	lists.apache.org text/html	MLIST [rocketmq-dev] 20190801 [GitHub] [rocketmq] duhenglucky commented on issue #1233: TLS Client-initiated renegotiation attack (CVE-2011-1473)
Re: [TLS] SSL Renegotiation DOS	www.ietf.org text/html	MLIST [tls] 20110315 Re: SSL Renegotiation DOS
SSL Renegotiation Denial of Service ‹ Jorge Orchilles	web.archive.org text/html Inactive Link Not Archived	MISC orchilles.com/2011/03/ssl-renegotiation-dos.html
No Description Provided	archives.neohapsis.com Inactive Link Not Archived	BUGTRAQ 20140214 ESA-2014-009: RSA BSAFE SSL-J Multiple Vulnerabilities
'[security bulletin] HPSBMU02776 SSRT100852 rev.1 - HP Onboard Administrator (OA), Remote Unauthorize' - MARC	marc.info text/html	HP SSRT100852
oss-security - SSL renegotiation DoS CVE-2011-1473	www.openwall.com text/html	MLIST [oss-security] 20110708 SSL renegotiation DoS CVE-2011-1473
Pony Mail!	lists.apache.org text/html	MLIST [rocketmq-dev] 20210311 [GitHub] [rocketmq] mouzz commented on pull request #1820: [ISSUE #1233] Fix CVE-2011-1473
Pony Mail!	lists.apache.org text/html	MLIST [rocketmq-dev] 20200305 [GitHub] [rocketmq] ShadowySpirits commented on issue #1233: TLS Client-initiated renegotiation attack (CVE-2011-1473)

Pony Mail!	lists.apache.org text/html	MLIST [rocketmq-dev] 20200305 [GitHub] [rocketmq] coveralls commented on issue #1820: [ISSUE #1233] Fix CVE-2011-1473
Pony Mail!	lists.apache.org text/html	MLIST [rocketmq-dev] 20190527 [GitHub] [rocketmq] bix29 opened a new issue #1233: TLS Client-initiated renegotiation attack (CVE-2011-1473)

There are currently no QIDs associated with this CVE

Exploit/POC from Github

A bash script that attempts to flood a server with TLS renegotiations by using the openssl client. See CVE-2011-1473 …

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Openssl	Openssl	0.9.8m	All	All	All
Application	Openssl	Openssl	0.9.8m	beta1	All	All
Application	Openssl	Openssl	0.9.8n	All	All	All
Application	Openssl	Openssl	0.9.8o	All	All	All
Application	Openssl	Openssl	0.9.8p	All	All	All
Application	Openssl	Openssl	0.9.8r	All	All	All
Application	Openssl	Openssl	0.9.8s	All	All	All
Application	Openssl	Openssl	0.9.8t	All	All	All
Application	Openssl	Openssl	0.9.8u	All	All	All
Application	Openssl	Openssl	0.9.8v	All	All	All
Application	Openssl	Openssl	0.9.8w	All	All	All
Application	Openssl	Openssl	0.9.8x	All	All	All
Application	Openssl	Openssl	All	All	All	All
Application	Openssl	Openssl	0.9.8m	All	All	All
Application	Openssl	Openssl	0.9.8m	beta1	All	All
Application	Openssl	Openssl	0.9.8n	All	All	All
Application	Openssl	Openssl	0.9.8o	All	All	All
Application	Openssl	Openssl	0.9.8p	All	All	All
Application	Openssl	Openssl	0.9.8r	All	All	All
Application	Openssl	Openssl	0.9.8s	All	All	All

Application	Openssl	Openssl	0.9.8t	All	All	All
Application	Openssl	Openssl	0.9.8u	All	All	All
Application	Openssl	Openssl	0.9.8v	All	All	All
Application	Openssl	Openssl	0.9.8w	All	All	All
Application	Openssl	Openssl	0.9.8x	All	All	All

cpe:2.3:a:openssl:openssl:0.9.8m:*:*:*:*:*:*:*:

cpe:2.3:a:openssl:openssl:0.9.8m:beta1:*:*:*:*:*:*:

cpe:2.3:a:openssl:openssl:0.9.8n:*:*:*:*:*:*:*:

cpe:2.3:a:openssl:openssl:0.9.8o:*:*:*:*:*:*:*:

cpe:2.3:a:openssl:openssl:0.9.8p:*:*:*:*:*:*:*:

cpe:2.3:a:openssl:openssl:0.9.8r:*:*:*:*:*:*:*:

cpe:2.3:a:openssl:openssl:0.9.8s:*:*:*:*:*:*:*:

cpe:2.3:a:openssl:openssl:0.9.8t:*:*:*:*:*:*:*:

cpe:2.3:a:openssl:openssl:0.9.8u:*:*:*:*:*:*:*:

cpe:2.3:a:openssl:openssl:0.9.8v:*:*:*:*:*:*:*:

cpe:2.3:a:openssl:openssl:0.9.8w:*:*:*:*:*:*:*:

cpe:2.3:a:openssl:openssl:0.9.8x:*:*:*:*:*:*:*:

cpe:2.3:a:openssl:openssl:*:*:*:*:*:*:*:*:

cpe:2.3:a:openssl:openssl:0.9.8m:*:*:*:*:*:*:*:

cpe:2.3:a:openssl:openssl:0.9.8m:beta1:*:*:*:*:*:*:

cpe:2.3:a:openssl:openssl:0.9.8n:*:*:*:*:*:*:*:

cpe:2.3:a:openssl:openssl:0.9.8o:*:*:*:*:*:*:*:

cpe:2.3:a:openssl:openssl:0.9.8p:*:*:*:*:*:*:*:

cpe:2.3:a:openssl:openssl:0.9.8r:*:*:*:*:*:*:*:

cpe:2.3:a:openssl:openssl:0.9.8s:*:*:*:*:*:*:*:

cpe:2.3:a:openssl:openssl:0.9.8t:*:*:*:*:*:*:*:

cpe:2.3:a:openssl:openssl:0.9.8u:*:*:*:*:*:*:*:

cpe:2.3:a:openssl:openssl:0.9.8v:*:*:*:*:*:*:*:

cpe:2.3:a:openssl:openssl:0.9.8w:*:*:*:*:*:*:*:

cpe:2.3:a:openssl:openssl:0.9.8x:*:*:*:*:*:*:*:

cpe:2.3:a:openssl:openssl:0.9.8x: . . . . . .

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
/r/oscp	Exploit SSL/TLS renegotiation is NOT enabled	2020-08-24 01:48:38
/r/ethicalhacking	Exploit SSL/TLS renegotiation is NOT enabled	2020-08-24 01:43:13

← Previous ID

Next ID→