



CVE-2011-5094

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

Last Modified on: 11/07/2023 02:09:00 AM UTC

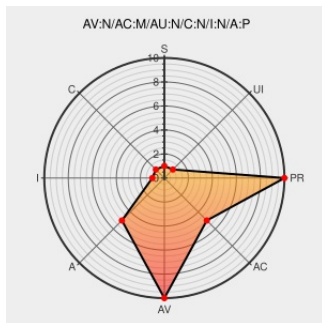
CVE-2011-5094

[Source: Mitre](#)

[Source: NIST](#)

[CVE.ORG](#)

[Print: PDF](#)



Certain versions of [Network Security Services](#) from [Mozilla](#) contain the following vulnerability:

**** DISPUTED **** Mozilla Network Security Services (NSS) 3.x, with certain settings of the `SSL_ENABLE_RENEGOTIATION` option, 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-2011-1473.

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-2011-5094 has been assigned by [M](#) cve@mitre.org to track the vulnerability

CVSS2 Score: **4.3 - MEDIUM**

Access
Vector

NETWORK

Access
Complexity

MEDIUM

Authentication

NONE

Confidentiality
Impact

NONE

Integrity
Impact

NONE

Availability
Impact

PARTIAL

CVE References

Description

Tags

Link

Re: [TLS] SSL Renegotiation
DOS

www.ietf.org
[text/html](#)

[MLIST \[tls\] 20110315 Re: SSL Renegotiation DOS](#)

707065 – (CVE-2011-1473) CVE-
2011-1473 openssl: DoS via
repeated SSL session
renegotiations

bugzilla.redhat.com
[text/html](#)

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
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
SSL/TLS and Computational DoS - Educated Guesswork	www.educatedguesswork.org text/html	 MISC www.educatedguesswork.org/2011/10/ssl_tls_and_computational_dos.html
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
oss-security - SSL renegotiation DoS CVE-2011-1473	www.openwall.com text/html	 MLIST [oss-security] 20110708 SSL renegotiation DoS CVE-2011-1473

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
Application	Mozilla	Network Security Services	3.11.2	All	All	All
Application	Mozilla	Network Security Services	3.11.3	All	All	All
Application	Mozilla	Network Security Services	3.11.4	All	All	All
Application	Mozilla	Network Security Services	3.11.5	All	All	All
Application	Mozilla	Network Security Services	3.2	All	All	All
Application	Mozilla	Network Security Services	3.2.1	All	All	All
Application	Mozilla	Network Security Services	3.3	All	All	All
Application	Mozilla	Network Security Services	3.3.1	All	All	All
Application	Mozilla	Network Security Services	3.3.2	All	All	All
Application	Mozilla	Network Security Services	3.4	All	All	All
Application	Mozilla	Network Security Services	3.4.1	All	All	All
Application	Mozilla	Network Security Services	3.4.2	All	All	All
Application	Mozilla	Network Security Services	3.5	All	All	All
Application	Mozilla	Network Security Services	3.6	All	All	All
Application	Mozilla	Network Security Services	3.6.1	All	All	All
Application	Mozilla	Network Security Services	3.7	All	All	All

Application	Mozilla	Network Security Services	3.7.1	All	All	All
Application	Mozilla	Network Security Services	3.7.2	All	All	All
Application	Mozilla	Network Security Services	3.7.3	All	All	All
Application	Mozilla	Network Security Services	3.7.5	All	All	All
Application	Mozilla	Network Security Services	3.7.7	All	All	All
Application	Mozilla	Network Security Services	3.8	All	All	All
Application	Mozilla	Network Security Services	3.9	All	All	All
Application	Mozilla	Network Security Services	3.11.2	All	All	All
Application	Mozilla	Network Security Services	3.11.3	All	All	All
Application	Mozilla	Network Security Services	3.11.4	All	All	All
Application	Mozilla	Network Security Services	3.11.5	All	All	All
Application	Mozilla	Network Security Services	3.2	All	All	All
Application	Mozilla	Network Security Services	3.2.1	All	All	All
Application	Mozilla	Network Security Services	3.3	All	All	All
Application	Mozilla	Network Security Services	3.3.1	All	All	All
Application	Mozilla	Network Security Services	3.3.2	All	All	All
Application	Mozilla	Network Security Services	3.4	All	All	All
Application	Mozilla	Network Security Services	3.4.1	All	All	All
Application	Mozilla	Network Security Services	3.4.2	All	All	All
Application	Mozilla	Network Security Services	3.5	All	All	All
Application	Mozilla	Network Security Services	3.6	All	All	All
Application	Mozilla	Network Security Services	3.6.1	All	All	All
Application	Mozilla	Network Security Services	3.7	All	All	All
Application	Mozilla	Network Security Services	3.7.1	All	All	All
Application	Mozilla	Network Security Services	3.7.2	All	All	All
Application	Mozilla	Network Security Services	3.7.3	All	All	All
Application	Mozilla	Network Security Services	3.7.5	All	All	All
Application	Mozilla	Network Security Services	3.7.7	All	All	All
Application	Mozilla	Network Security Services	3.8	All	All	All
Application	Mozilla	Network Security Services	3.9	All	All	All
cpe:2.3:a:mozilla:network_security_services:3.11.2:*:*:*:*:*:						
cpe:2.3:a:mozilla:network_security_services:3.11.3:*:*:*:*:*:						
cpe:2.3:a:mozilla:network_security_services:3.11.4:*:*:*:*:*:						
cpe:2.3:a:mozilla:network_security_services:3.11.5:*:*:*:*:*:						
cpe:2.3:a:mozilla:network_security_services:3.2:*:*:*:*:*:						

cpe:2.3:a:mozilla:network_security_services:3.2:*****:
cpe:2.3:a:mozilla:network_security_services:3.2.1:*****:
cpe:2.3:a:mozilla:network_security_services:3.3:*****:
cpe:2.3:a:mozilla:network_security_services:3.3.1:*****:
cpe:2.3:a:mozilla:network_security_services:3.3.2:*****:
cpe:2.3:a:mozilla:network_security_services:3.4:*****:
cpe:2.3:a:mozilla:network_security_services:3.4.1:*****:
cpe:2.3:a:mozilla:network_security_services:3.4.2:*****:
cpe:2.3:a:mozilla:network_security_services:3.5:*****:
cpe:2.3:a:mozilla:network_security_services:3.6:*****:
cpe:2.3:a:mozilla:network_security_services:3.6.1:*****:
cpe:2.3:a:mozilla:network_security_services:3.7:*****:
cpe:2.3:a:mozilla:network_security_services:3.7.1:*****:
cpe:2.3:a:mozilla:network_security_services:3.7.2:*****:
cpe:2.3:a:mozilla:network_security_services:3.7.3:*****:
cpe:2.3:a:mozilla:network_security_services:3.7.5:*****:
cpe:2.3:a:mozilla:network_security_services:3.7.7:*****:
cpe:2.3:a:mozilla:network_security_services:3.8:*****:
cpe:2.3:a:mozilla:network_security_services:3.9:*****:
cpe:2.3:a:mozilla:network_security_services:3.11.2:*****:
cpe:2.3:a:mozilla:network_security_services:3.11.3:*****:
cpe:2.3:a:mozilla:network_security_services:3.11.4:*****:
cpe:2.3:a:mozilla:network_security_services:3.11.5:*****:
cpe:2.3:a:mozilla:network_security_services:3.2:*****:
cpe:2.3:a:mozilla:network_security_services:3.2.1:*****:
cpe:2.3:a:mozilla:network_security_services:3.3:*****:
cpe:2.3:a:mozilla:network_security_services:3.3.1:*****:
cpe:2.3:a:mozilla:network_security_services:3.3.2:*****:
cpe:2.3:a:mozilla:network_security_services:3.4:*****:

cpe:2.3:a:mozilla:network_security_services:3.4.1:~::~~::~~::~~::~~::~~::
cpe:2.3:a:mozilla:network_security_services:3.4.2:~::~~::~~::~~::~~::~~::
cpe:2.3:a:mozilla:network_security_services:3.5:~::~~::~~::~~::~~::~~::
cpe:2.3:a:mozilla:network_security_services:3.6:~::~~::~~::~~::~~::~~::
cpe:2.3:a:mozilla:network_security_services:3.6.1:~::~~::~~::~~::~~::~~::
cpe:2.3:a:mozilla:network_security_services:3.7:~::~~::~~::~~::~~::~~::
cpe:2.3:a:mozilla:network_security_services:3.7.1:~::~~::~~::~~::~~::~~::
cpe:2.3:a:mozilla:network_security_services:3.7.2:~::~~::~~::~~::~~::~~::
cpe:2.3:a:mozilla:network_security_services:3.7.3:~::~~::~~::~~::~~::~~::
cpe:2.3:a:mozilla:network_security_services:3.7.5:~::~~::~~::~~::~~::~~::
cpe:2.3:a:mozilla:network_security_services:3.7.7:~::~~::~~::~~::~~::~~::
cpe:2.3:a:mozilla:network_security_services:3.8:~::~~::~~::~~::~~::~~::
cpe:2.3:a:mozilla:network_security_services:3.9:~::~~::~~::~~::~~::~~::

No vendor comments have been submitted for this CVE

[← Previous ID](#)

[Next ID →](#)