



CVE-2014-3604

Published on: 10/24/2014 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:25:46 PM UTC

CVE-2014-3604

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

Certain versions of [Not Yet Commons Ssl](#) from [Not Yet Commons Ssl Project](#) contain the following vulnerability:

Certificates.java in Not Yet Commons SSL before 0.3.15 does not properly verify that the server hostname matches a domain name in the subject's Common Name (CN) field of the X.509 certificate, which allows man-in-the-middle attackers to spoof SSL servers via an arbitrary valid certificate.

CVE-2014-3604 has been assigned by secalert@redhat.com to track the vulnerability

CVSS2 Score: **6.8 - MEDIUM**

Access
Vector

NETWORK

Access
Complexity

MEDIUM

Authentication

NONE

Confidentiality
Impact

PARTIAL

Integrity
Impact

PARTIAL

Availability
Impact

PARTIAL

CVE References

Description

Tags

Link

Red Hat Customer Portal

[web.archive.org](#)

[text/html](#)

[Inactive Link](#) [Not Archived](#)

[REDHAT RHSA-2015:1888](#)

IBM X-Force Exchange

[exchange.xforce.ibmcloud.com](#)

[text/html](#)

[XF notyetcommons-cve20143604-sec-bypass\(97659\)](#)

404 Not Found

[Patch](#)

[juliusdavies.ca](#)

[text/html](#)

[Inactive Link](#) [Not Archived](#)

[CONFIRM](#)
[juliusdavies.ca/svn/viewvc.cgi/not-yet-commons-ssl?view=rev&revision=172](#)

Bug 1131803 – CVE-2014-3604 Not Yet Commons SSL: Hostname verification susceptible to MITM attack

[bugzilla.redhat.com](#)

[text/html](#)

[MISC bugzilla.redhat.com/show_bug.cgi?id=1131803](#)

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	Not Yet Commons Ssl Project	Not Yet Commons Ssl	All	All	All	All
cpe:2.3:a:not_yet_commons_ssl_project:not_yet_commons_ssl:*****:						

No vendor comments have been submitted for this CVE

[← Previous ID](#)

[Next ID →](#)