



# CVE-2014-3577

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF !\[\]\(e3f8612927870f2e0f9f5989e6dd3064\_img.jpg\)](#)

## Summary

<b>CVE</b>	CVE-2014-3577
<b>State</b>	PUBLIC
<b>Assigner</b>	secalert@redhat.com
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2014-08-21 14:55:00 UTC
<b>Updated</b>	2023-11-07 02:20:00 UTC
<b>Description</b>	org.apache.http.conn.ssl.AbstractVerifier in Apache HttpComponents HttpClient before 4.3.5 and HttpAsyncClient before 4.

## Risk And Classification

**Problem Types:** NVD-CWE-Other

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	<a href="#">Apache</a>	<a href="#">Httpasyncclient</a>	All	All	All	All
Application	<a href="#">Apache</a>	<a href="#">HttpClient</a>	All	All	All	All

## References

### Reference

- Full Disclosure: CVE-2014-3577: Apache HttpComponents client: Hostname verification susceptible to MITM attack
- Red Hat Customer Portal
- Security Advisory SA60713 - Apache HttpComponents HttpClient / Apache HttpComponents HttpAsyncClient X.509 Certificate Validation Sec
- Document Display | HPE Support Center
- Red Hat Customer Portal
- Pony Mail!
- Red Hat Customer Portal
- Apache HttpComponents Man-In-The-Middle ≈ Packet Storm
- [security-announce] openSUSE-SU-2020:1873-1: important: Security update
- [cxf-commits] 20210402 svn commit: r1073270 - in /websites/production/cxf/content: cache/main.pageCache security-advisories.data/CVE-20:
- Pony Mail!
- Red Hat Customer Portal

Pony Mail!
IBM X-Force Exchange
USN-2769-1: Apache Commons HttpClient vulnerabilities   Ubuntu
Red Hat Customer Portal
Red Hat Customer Portal
CPU July 2018
Pony Mail!
Red Hat Customer Portal
oss-security - Multiple vulnerabilities in Jenkins and Jenkins plugins
Pony Mail!
Pony Mail!
Apache HttpComponents Incomplete Fix CVE-2014-3577 SSL Validation Security Bypass Vulnerability
Do CVE-2012-6153 and CVE-2014-3577 affect Red Hat products? - Red Hat Customer Portal
110143
Red Hat Customer Portal
Pony Mail!
Red Hat Customer Portal
Security Advisory SA60589 - Red Hat update for httpcomponents-client - Secunia
Red Hat JBoss Certificate Validation Flaw Lets Remote Users Spoof SSL Servers - SecurityTracker
About Secunia Research   Flexera
Pony Mail!
[cxf-commits] 20210616 svn commit: r1075801 - in /websites/production/cxf/content: cache/main.pageCache index.html security-advisories.da
Document Display   HPE Support Center
Red Hat Customer Portal
Pony Mail!
Red Hat Customer Portal
Pony Mail!
Red Hat Customer Portal
[security-announce] openSUSE-SU-2020:1875-1: important: Security update
Pony Mail!
CVE-2014-3577 Apache HttpComponents HttpClient Vulnerability in NetApp Products   NetApp Product Security
Red Hat Customer Portal
Red Hat Customer Portal
Red Hat Customer Portal
Pony Mail!

Red Hat Customer Portal
Pony Mail!
Pony Mail!
Red Hat Customer Portal
Pony Mail!
Red Hat Customer Portal
Red Hat Customer Portal
Red Hat Customer Portal
Pony Mail!
CVE Program record
NVD vulnerability detail

No vendor comments have been submitted for this CVE.

### Legacy QID Mappings

<a href="#">20269</a> IBM DB2 Multiple Vulnerabilities (6466365)
<a href="#">20330</a> IBM DB2 Secure Sockets Layer (SSL) Server Spoofing Vulnerability (6953757)
<a href="#">240138</a> Red Hat OpenShift Container Platform 4.1 Security Update (RHSA-2022:0055)
<a href="#">375670</a> IBM WebSphere Application Server Multiple Vulnerabilities (6453091)
<a href="#">690202</a> Free Berkeley Software Distribution (FreeBSD) Security Update for jenkins (9bad457e-b396-4452-8773-15bec67e1ceb)
<a href="#">730235</a> Jenkins Core Security Update (Jenkins Security Advisory 2021-10-06)
<a href="#">770138</a> Red Hat OpenShift Container Platform 4.1 Security Update (RHSA-2022:0055)
<a href="#">980486</a> Java (maven) Security Update for org.apache.httpcomponents:httpClient (GHSA-cfh5-3ghh-wfjx)

© [CVE.report](#) 2026 |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

**CVE.report and Source URL Uptime Status [status.cve.report](#)**