



# CVE-2017-9735

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

## Summary

<b>CVE</b>	CVE-2017-9735
<b>State</b>	PUBLIC
<b>Assigner</b>	cve@mitre.org
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2017-06-16 21:29:00 UTC
<b>Updated</b>	2023-11-07 02:50:00 UTC
<b>Description</b>	Jetty through 9.4.x is prone to a timing channel in util/security/Password.java, which makes it easier for remote attackers to

## Risk And Classification

### Problem Types: CWE-203

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Debian	Debian Linux	9.0	All	All	All
Application	Eclipse	Jetty	All	All	All	All
Application	Eclipse	Jetty	All	20170531	All	All
Application	Oracle	Communications Cloud Native Core Policy	1.5.0	All	All	All
Application	Oracle	Enterprise Manager Base Platform	13.2	All	All	All
Application	Oracle	Enterprise Manager Base Platform	13.3	All	All	All
Application	Oracle	Hospitality Guest Access	4.2.0	All	All	All
Application	Oracle	Hospitality Guest Access	4.2.1	All	All	All
Application	Oracle	Rest Data Services	11.2.0.4	All	All	All
Application	Oracle	Rest Data Services	12.1.0.2	All	All	All
Application	Oracle	Rest Data Services	12.2.0.1	All	All	All
Application	Oracle	Rest Data Services	18c	All	All	All
Application	Oracle	Retail Xstore Point Of Service	15.0	All	All	All
Application	Oracle	Retail Xstore Point Of Service	16.0	All	All	All
Application	Oracle	Retail Xstore Point Of Service	17.0	All	All	All
Application	Oracle	Retail Xstore Point Of Service	7.1	All	All	All

References				
Reference	Source	Link	Tags	
Pony Mail!		<a href="https://lists.apache.org">lists.apache.org</a>		
[SECURITY] [DLA 2661-1] jetty9 security update	MLIST	<a href="https://lists.debian.org">lists.debian.org</a>		
#864631 - unblock: jetty9/9.2.22-1 - Debian Bug report logs	MISC	<a href="https://bugs.debian.org">bugs.debian.org</a>	Mailing	
Pony Mail!		<a href="https://lists.apache.org">lists.apache.org</a>		
Pony Mail!	MLIST	<a href="https://lists.apache.org">lists.apache.org</a>		
Oracle Critical Patch Update Advisory - October 2020	MISC	<a href="https://www.oracle.com">www.oracle.com</a>		
Oracle Critical Patch Update Advisory - July 2021	N/A	<a href="https://www.oracle.com">www.oracle.com</a>		
Pony Mail!	MLIST	<a href="https://lists.apache.org">lists.apache.org</a>		
Pony Mail!		<a href="https://lists.apache.org">lists.apache.org</a>		
Pony Mail!		<a href="https://lists.apache.org">lists.apache.org</a>		
Pony Mail!	MLIST	<a href="https://lists.apache.org">lists.apache.org</a>		
Pony Mail!		<a href="https://lists.apache.org">lists.apache.org</a>		
Remove a timing channel in Password matching · Issue #1556 · eclipse/jetty.project · GitHub	MISC	<a href="https://github.com">github.com</a>	Third P	
Pony Mail!	MLIST	<a href="https://lists.apache.org">lists.apache.org</a>		
Pony Mail!	MLIST	<a href="https://lists.apache.org">lists.apache.org</a>		
Oracle Critical Patch Update - October 2019	MISC	<a href="https://www.oracle.com">www.oracle.com</a>		
Pony Mail!		<a href="https://lists.apache.org">lists.apache.org</a>		
Pony Mail!	MLIST	<a href="https://lists.apache.org">lists.apache.org</a>		
Malformed Request	BID	<a href="https://www.securityfocus.com">www.securityfocus.com</a>	Third P	
CVE Program record	CVE.ORG	<a href="https://www.cve.org">www.cve.org</a>	canonic	
NVD vulnerability detail	NVD	<a href="https://nvd.nist.gov">nvd.nist.gov</a>	canonic	

No vendor comments have been submitted for this CVE.

### Legacy QID Mappings

[178597](#) Debian Security Update for jetty9 (DLA 2661-1)

[982326](#) Java (maven) Security Update for org.eclipse.jetty:jetty-server (GHSA-wfcc-pff6-rgc5)

© 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](#).

