



CVE-2021-22160

Published on: 05/26/2021 12:00:00 AM UTC

Last Modified on: 06/04/2022 02:49:00 AM UTC

CVE-2021-22160

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

CVSS:31/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H



Certain versions of [Pulsar](#) from [Apache](#) contain the following vulnerability:

If Apache Pulsar is configured to authenticate clients using tokens based on JSON Web Tokens (JWT), the signature of the token is not validated if the algorithm of the presented token is set to "none". This allows an attacker to connect to Pulsar instances as any user (incl. admins).

CVE-2021-22160 has been assigned by security@apache.org to track the vulnerability - currently rated as **CRITICAL** severity.

Affected Vendor/Software: **Apache Software Foundation - Apache Pulsar** version < 2.7.1

CVSS3 Score: **9.8 - CRITICAL**

Attack Vector	Attack Complexity	Privileges Required	User Interaction
NETWORK	LOW	NONE	NONE
Scope	Confidentiality Impact	Integrity Impact	Availability Impact
UNCHANGED	HIGH	HIGH	HIGH

CVSS2 Score: **7.5 - HIGH**

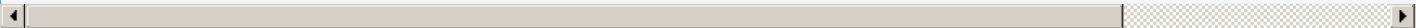
Access Vector	Access Complexity	Authentication
NETWORK	LOW	NONE
Confidentiality Impact	Integrity Impact	Availability Impact
PARTIAL	PARTIAL	PARTIAL

CVE References

Description	Tags	Link
Pony Mail!	lists.apache.org	MLIST [pulsar-dev] 20210528 Re: Cutting 2.6.4 release to address CVE-2021-22160

	text/html	
Pony Mail!	lists.apache.org text/html	MLIST Re: [SECURITY] [CVE-2021-22160] Authentication with JWT allows use of "none"-algorithm
Pony Mail!	lists.apache.org text/html	MISC lists.apache.org/thread.html/r347650d15a3e9c5f58b83e918b6ad6dedc2a63d3eb63da8e6a7be87e%40%3C
Pony Mail!	lists.apache.org text/html	MLIST [pulsar-commits] 20210528 [GitHub] [pulsar] lhotari commented on issue #10733: Pulsar 2.6.3 JW persistent/public/default 401 error
Pony Mail!	lists.apache.org text/html	MLIST [pulsar-users] 20210527 Re: [SECURITY] [CVE-2021-22160] Authentication with JWT allows use
Pony Mail!	lists.apache.org text/html	MLIST [pulsar-commits] 20210528 [GitHub] [pulsar] lhotari edited a comment on issue #10733: Pulsar 2.6 /admin/v2/non-persistent/public/default 401 error
Pony Mail!	lists.apache.org text/html	MLIST [pulsar-dev] 20210527 Re: [SECURITY] [CVE-2021-22160] Authentication with JWT allows use of
Pony Mail!	lists.apache.org text/html	MLIST [pulsar-dev] 20210527 Re: Cutting 2.6.4 release to address CVE-2021-22160
Pony Mail!	lists.apache.org text/html	MLIST [pulsar-dev] 20210604 Re: [DISCUSS] Propose More Formal Policy for Security Patches and EOL
Pony Mail!	lists.apache.org text/html	MLIST [pulsar-dev] 20210527 Cutting 2.6.4 release to address CVE-2021-22160
Pony Mail!	lists.apache.org text/html	MLIST [pulsar-dev] 20210531 Re: [DISCUSS] Propose More Formal Policy for Security Patches and EOL

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.



Related QID Numbers

982355 Java (maven) Security Update for org.apache.pulsar:pulsar (GHSA-3cv4-xxv7-934q)

Known Affected Configurations (CPE V2.3)						
Type	Vendor	Product	Version	Update	Edition	Language
Application	Apache	Pulsar	All	All	All	All
cpe:2.3:a:apache:pulsar:*:*:*:*:*:						

No vendor comments have been submitted for this CVE

Social Mentions		
Source	Title	Posted (UTC)
@CVEreport	CVE-2021-22160 : If #Apache Pulsar is configured to authenticate clients using tokens based on JSON Web Tokens JWT... twitter.com/i/web/status/1...	2021-05-26 12:28:48
@ulldma	The counter on the site howmanydayssinceajwtalgnonevuln.com had to be reset to zero. Sorry about that! (CVE-2021-22160) https://t.co/ZCNB8u3DpU	2021-05-26 17:12:42

[← Previous ID](#)[Next ID→](#)© [CVE.report](#) 2023   |

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](#)