



CVE-2020-17516

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF !\[\]\(e3f8612927870f2e0f9f5989e6dd3064_img.jpg\)](#)

Summary

CVE	CVE-2020-17516
State	PUBLIC
Assigner	security@apache.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2021-02-03 17:15:00 UTC
Updated	2023-11-07 03:19:00 UTC
Description	Apache Cassandra versions 2.1.0 to 2.1.22, 2.2.0 to 2.2.19, 3.0.0 to 3.0.23, and 3.11.0 to 3.11.9, when using 'dc' or 'rack' in

Risk And Classification

Problem Types: CWE-290

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Apache	Cassandra	All	All	All	All
Application	Apache	Cassandra	All	All	All	All
Application	Apache	Cassandra	All	All	All	All
Application	Apache	Cassandra	All	All	All	All

References

Reference	Source	Link
[CVE-2020-17516] Apache Cassandra internode encryption enforcement vulnerability		mail-archive
CVE-2020-17516 Apache Cassandra Vulnerability in NetApp Products NetApp Product Security	CONFIRM	security.net
Pony Mail!	MLIST	lists.apache
[cassandra-commits] 20210915 [jira] [Updated] (CASSANDRA-16455) CVE-2020-17516 mitigation in 2.2.x branch		lists.apache
[CVE-2020-17516] Apache Cassandra internode encryption enforcement vulnerability	CONFIRM	mail-archive
Pony Mail!	MLIST	lists.apache
[cassandra-commits] 20210523 [jira] [Updated] (CASSANDRA-16455) CVE-2020-17516 mitigation in 2.2.x branch		lists.apache
Pony Mail!		lists.apache
Pony Mail!	MLIST	lists.apache
CVE Program record	CVE.ORG	www.cve.or

No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.

© [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](#)