



# CVE-2020-13946

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF](#)

## Summary

<b>CVE</b>	CVE-2020-13946
<b>State</b>	PUBLIC
<b>Assigner</b>	security@apache.org
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2020-09-01 21:15:00 UTC
<b>Updated</b>	2023-11-07 03:17:00 UTC
<b>Description</b>	In Apache Cassandra, all versions prior to 2.1.22, 2.2.18, 3.0.22, 3.11.8 and 4.0-beta2, it is possible for a local attacker with

## Risk And Classification

**Problem Types:** CWE-668

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	<a href="#">Apache</a>	<a href="#">Cassandra</a>	All	All	All	All
Application	<a href="#">Apache</a>	<a href="#">Cassandra</a>	4.0.0	alpha1	All	All
Application	<a href="#">Apache</a>	<a href="#">Cassandra</a>	4.0.0	alpha2	All	All
Application	<a href="#">Apache</a>	<a href="#">Cassandra</a>	4.0.0	alpha3	All	All
Application	<a href="#">Apache</a>	<a href="#">Cassandra</a>	4.0.0	alpha4	All	All
Application	<a href="#">Apache</a>	<a href="#">Cassandra</a>	4.0.0	beta1	All	All
Application	<a href="#">Apache</a>	<a href="#">Cassandra</a>	All	All	All	All
Application	<a href="#">Apache</a>	<a href="#">Cassandra</a>	4.0.0	alpha1	All	All
Application	<a href="#">Apache</a>	<a href="#">Cassandra</a>	4.0.0	alpha2	All	All
Application	<a href="#">Apache</a>	<a href="#">Cassandra</a>	4.0.0	alpha3	All	All
Application	<a href="#">Apache</a>	<a href="#">Cassandra</a>	4.0.0	alpha4	All	All
Application	<a href="#">Apache</a>	<a href="#">Cassandra</a>	4.0.0	beta1	All	All
Application	<a href="#">Netapp</a>	<a href="#">Oncommand Insight</a>	-	All	All	All

## References

Reference	Source	Link	Tags
Pony Mail!	MLIST	<a href="mailto:lists.apache.org">lists.apache.org</a>	Mailin

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>	
CVE-2020-13946 Apache Cassandra Vulnerability in NetApp Products   NetApp Product Security		CONFIRM	<a href="https://security.netapp.com">security.netapp.com</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>	Mailin
Pony Mail!		MISC	<a href="https://lists.apache.org">lists.apache.org</a>	Mailin
CVE Program record		CVE.ORG	<a href="https://www.cve.org">www.cve.org</a>	canon
NVD vulnerability detail		NVD	<a href="https://nvd.nist.gov">nvd.nist.gov</a>	canon

No vendor comments have been submitted for this CVE.

### Legacy QID Mappings

[982396](#) Java (maven) Security Update for org.apache.cassandra:cassandra-all (GHSA-24ww-mc5x-xc43)

© [CVE.report](https://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](https://mitre.org) and the authoritative source of CVE content is [MITRE's CVE web site](https://mitre.org/cve). This site includes MITRE data granted under the following [license](#).

**CVE.report and Source URL Uptime Status** [status.cve.report](https://status.cve.report)