



# CVE-2022-26133

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

## Summary

<b>CVE</b>	CVE-2022-26133
<b>State</b>	PUBLIC
<b>Assigner</b>	security@atlassian.com
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2022-04-20 19:15:00 UTC
<b>Updated</b>	2022-04-28 17:50:00 UTC
<b>Description</b>	SharedSecretClusterAuthenticator in Atlassian Bitbucket Data Center versions 5.14.0 and later before 7.6.14, 7.7.0 and later

## Risk And Classification

**Problem Types:** CWE-502

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	<a href="#">Atlassian</a>	<a href="#">Bitbucket Data Center</a>	All	All	All	All
Application	<a href="#">Atlassian</a>	<a href="#">Bitbucket Data Center</a>	7.20.0	All	All	All

## References

### Reference

- Multiple Products Security Advisory - Hazelcast Vulnerable To Remote Code Execution - CVE-2016-10750, CVE-2022-26133 | Atlassian Support
- [BSERV-13173] Bitbucket Data Center - Java Deserialization Vulnerability In Hazelcast - CVE-2022-26133 - Create and track feature requests
- CVE Program record
- NVD vulnerability detail

No vendor comments have been submitted for this CVE.

## Legacy QID Mappings

[376867](#) Atlassian Bitbucket Data Center Remote Code Execution (RCE) Vulnerability (BSERV-13173) (Authenticated Check)

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](#).

**Free CVE JSON API** [cve.report/api](#)

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