



CVE-2016-10750

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

Summary

CVE	CVE-2016-10750
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2019-05-22 14:29:00 UTC
Updated	2019-08-08 13:15:00 UTC
Description	In Hazelcast before 3.11, the cluster join procedure is vulnerable to remote code execution via Java deserialization. If an at

Risk And Classification

Problem Types: CWE-502

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Hazelcast	Hazelcast	All	All	All	All
Application	Hazelcast	Hazelcast	All	All	All	All

References

Reference

- Hazelcast is vulnerable to untrusted deserialization remote code execution · Issue #8024 · hazelcast/hazelcast · GitHub
- Add basic protection against untrusted deserialization by introducing blacklisting/whitelisting capabilities by kwart · Pull Request #12230 · haze
- Red Hat Customer Portal
- CVE Program record
- NVD vulnerability detail

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

[730424](#) Atlassian Bitbucket Data Center Remote Code Execution (RCE) Vulnerability

[730425](#) Atlassian Confluence Data Center Remote Code Execution (RCE) Vulnerability

[730544](#) Atlassian Confluence Data Center Remote Code Execution (RCE) Vulnerability (CONFIRMED 730425)

© [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](#).

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

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