Multiple Products Security Advisory - 2022-03-24

Contents

Date	24 Mar 2022
Product	• Bitbucket Data Center • Confluence Data Center
Vulnerability	Critical
CVE	CVE-2016-10750
Official link	Multiple Products Security Advisory - Hazelcast Vulnerable To Remote Code Execution - CVE-2016-10750

Multiple Products Security Advisory - Hazelcast Vulnerable To Remote Code Execution - CVE-2016-10750

Dear customer,

on the 24th March 2022 23:00 UTC, Atlassian issued a Security Advisory for Confluence and Bitbucket Data Center. The Server and Cloud versions of the aplications as well as other Atlassian products are not affected.

What you need to know

A vulnerability in the software Hazelcast has been discovered in conjunction with the named Atlassian products. Hazelcast is used by Confluence and Bitbucket Data Center when configured to operate as a cluster. A remote, unauthenticated attacker can exploit this vulnerability.

Affected Versions

ⓘ

- Confluence Server and Cloud are **not** affected.
- Confluence Data Center instances that are **not installed as a cluster** are **not** affected.
- Bitbucket Server and Cloud are **not** affected.

Confluence Data Center

To verify whether a cluster installation is being used, check the `confluence.cfg.xml` file in the Confluence home directory. If the following line is present, it has been installed as a cluster:

confluence.cfg.xml

```
<property name="confluence.cluster">true</property>
```

If the line is not present *or* if the value is set to `false` instead of `true`, it has **not** been installed as a cluster.

The following versions of Confluence Data Center are affected when clustering is enabled:

- All versions 5.6.x and later

Bitbucket Data Center

Both single and multi-node installations of Bitbucket Data Center are affected. Enabling or disabling clustering does not affect whether or not the application is vulnerable.

The following versions of Bitbucket Data Center are affected:

- All 5.x versions before 5.14.x
- All 6.x versions
- All 7.x versions lower than 7.6.14

- All versions 7.7.x through 7.16.x
- 7.17.x lower than 7.17.6
- 7.18.x lower than 7.18.4
- 7.19.x lower than 7.19.4
- 7.20.0

What should I do?

Fix Confluence Data Center

Clustered
You installed Confluence Data Center clustered

Atlassian plans to address this security vulnerability in future releases, for now we recommend to apply the workaround.

Update

> ⓘ There is no Confluence release addressing this security vulnerability yet.

bitvoodoo will update this page with any news. To get notified as soon a Confluence Data Center version with fix get released, watch this issue:

- CONFSERVER-78179

Workaround

Restrict access to the Hazelcast port by using a firewall or other network access controls. The port only needs to be accessible by other nodes in the Bitbucket or Confluence cluster.

For Confluence Data Center, Hazelcast uses both TCP ports 5701 and 5801 by default.
Single node
You installed Confluence Data Center with clustering not enabled on a single node

> ✓ Single node installation of Confluence Data Center are not affected by this security vulnerability as Hazlecast is not utilized.

No need for action.

bitvoodoo Cloud
Confluence Data Center is hosted with bitvoodoo

> ✓ We have checked our installations according to the information in the Security Advisory and applied measures on network level. Your Confluence Data Center is secured.

No need for action.

Fix Bitbucket Data Center

Clustered
You run Bitbucket Data Center clustered on multiple nodes

Install a fixed version or apply the workaround as suggested by Atlassian.

Update

The following versions of Bitbucket Data Center fix this vulnerability:

- 7.6.14
- 7.17.6
- 7.18.4
- 7.19.4
- 7.20.1
- 7.21.0

Workaround

Restrict access to the Hazelcast port by using a firewall or other network access controls. The port only needs to be accessible by other nodes in the Bitbucket or Confluence cluster.

For Bitbucket Data Center, Hazelcast uses TCP port 5701 by default.
Single node
You run Bitbucket Data Center on a single node

Bitbucket Data Center is also affected when only one node is running. Install a fixed version or apply the workaround as suggested by Atlassian.

Update

The following versions of Bitbucket Data Center fix this vulnerability:

- 7.6.14
- 7.17.6
- 7.18.4
- 7.19.4
- 7.20.1
- 7.21.0

Workaround

Restrict access to the Hazelcast port by using a firewall or other network access controls. The port only needs to be accessible by other nodes in the Bitbucket or Confluence cluster.

For Bitbucket Data Center, Hazelcast uses TCP port 5701 by default.
bitvoodoo Cloud
Bitbucket Data Center is hosted with bitvoodoo

✓ We have checked our installations according to the information in the Security Advisory and applied measures on network level needed. Your Bitbucket Data Center is secured.

No need for action.

Further Reading

- CVE-2016-10750

Support

If you still have questions or concerns regarding this advisory, please contact the bitvoodoo support via support.bitvoodoo.ch.