Bitbucket Security Advisory - 2021-12-16

Contents

Date	16 Dec 2021
Product	• Bitbucket Data Center and Server
Vulnerability	Critical
CVE	CVE-2021-44228, CVE-2021-45046, CVE-2021-45105
Official link	Multiple Products Security Advisory - Log4j Vulnerable To Remote Code Execution - CVE-2021-44228

Log4Shell Information - bitvoodoo apps
Looking for information about bitvoodoo apps? Look here.

Dear customer,

On Thursday 16th December, Atlassian updated their Security Advisory on CVE-2021-44228 aka. Log4Shell. See Multiple Products Security Advisory - Log4j Vulnerable To Remote Code Execution - CVE-2021-44228.

According to new findings, some versions of Bitbucket Data Center and Server are affected by Log4Shell due to unused log4j-core present in some Bitbucket versions and the bundled Easticsearch.

What you need to know

A security vulnerability was discovered in Apache Log4j 2. Log4j is a popular logging package for Java.

This is a security issue affecting a broad range of software based upon Java. Atlassian products such as Bitbucket, Jira and Confluence run on Java and also utilize Log4j.

Affected versions and fixed versions

Bitbucket Data Center and Server

Bitbucket

Affected versions

- All versions < 6.10.16
- 7.x < 7.6.12
- Versions >= 7.7.0 and < 7.14.2
- 7.15.x < 7.15.3
- 7.16.x < 7.16.3
- 7.17.x < 7.17.4
- 7.18.x < 7.18.3
- 7.19

Fixed versions

- 6.10.16
- 7.6.12
- 7.14.2
- 7.15.3
- 7.16.3
- 7.17.4
- 7.18.3
- 7.19.1 or newer

What should I do?

self-hosted

You host your application yourself

Fix

Atlassian is unable to release an updated version of the *bundled* Elasticsearch version due to licensing changes for Elasticsearch versions later than 7.10. The mitigation is contained in the updates instead.

Atlassian recommends that you upgrade to the latest version. For a full description of the latest versions, see the release notes for your application:

- Bitbucket Server and Data Center release notes

You can download the latest version of your application from the download center:

- Download Bitbucket Server and Data Center

Mitigation

If you are unable to install an updated version of Bitbucket and are running the bundled Elasticsearch, make the following change as per Elastic security advisory ESA-2021-31:

> *The simplest remediation is to set the JVM option -Dlog4j2.formatMsgNoLookups=true and restart each node of the cluster. For Elasticsearch 5.6.11+, 6.4+, and 7.0+, this provides full protection against the RCE and information leak attacks.*

Restart Bitbucket Server after adding the following line to the bottom of the file **`$BITBUCKET_HOME/shared/search/jvm.options`**

```
-Dlog4j2.formatMsgNoLookups=true
```

Please contact our support if you need assistance.

bitvoodoo Cloud

Your application is hosted with bitvoodoo

bitvoodoo secured your Bitbucket by implementation of the mitigation on 16 Dec 2021 and has not identified compromised systems. Bitbucket hosted with bitvoodoo are **not** affected.

Atlassian Cloud

You use Bitbucket Cloud

Atlassian secured their cloud products and has not identified compromised systems. The on-demad applications and are **not** affected.

Further Reading

- Original publication by LunaSec
- CVE-2021-44228
- Atlassian FAQ for CVE-2021-44228, CVE-2021-45046 and CVE-2021-45105
- Elastic security advisory ESA-2021-31

Support

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

Betroffene Versionen und behobene Versionen nach Produkt