Log4Shell - bitvoodoo Security Advisory - 2021-12-13

Contents

Date	13 Dec 2021
Product	• Apache Log4j 2
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 9th December, developers and security researchers found a security vulnerability in Apache Log4j 2.

Update 13 Dec 2021 : Atlassian put out a Security Advisory for this exploit here: Multiple Products Security Advisory - Log4j Vulnerable To Remote Code Execution - CVE-2021-44228.

Update 16 Dec 2021 : Atlassian updated the Security Advisory to inform about a finding that shows that some Bitbucket Data Center and Server Versions are affected. We created a info page here: Bitbucket Security Advisory - 2021-12-16.

Update 17 Dec 2021 : Atlassian updated their FAQ with information regarding CVE 2021-45046, see here: FAQ for CVE-2021-44228 and CVE-2021-45046.

Update 20 Dec 2021 : Atlassian updated their FAQ with information regarding CVE-2021-45105, see here: FAQ for CVE-2021-44228, CVE-2021-45046 and CVE-2021-45105.

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 Jira and Confluence run on Java and also utilize Log4j.

Atlassian products

Bitbucket

The following informations refer to all products except for **Bitbucket Server and Data Center**. If you use Bitbucket please refer to Bitbucket Security Advisory - 2021-12-16.

Data Center and Server Products

Most Atlassian on-premise applications use an outdated version of Log4j and are **not affected** if you didn't modify Log4j yourself. See FAQ for CVE-2021-44228 and CVE-2021-45046.

Cloud Products

Atlassian secured their cloud products and has not identified compromised systems. The on-demad applications and are **not affected**. See FAQ for CVE-2021-44228 and CVE-2021-45046.

What should I do?

self-hosted

You host your application yourself

If you have never customized the settings of Log4j inside the Atlassian installation, you are on the safe side. As your Atlassian application uses the default configuration of Log4j, you are **not affected** by the exploit.

If you have set Log4j to work with JMS Appenders or are unsure, follow the instructions "How can I mitigate this exploit?" in the FAQ for CVE-2021-44228 and CVE-2021-45046.

Apps

Third-party apps can still pose a risk. Atlassian is reviewing all apps and informs the vendors it the find a security risk. We have checked our bitvoodoo apps and found them to be risk-free. You can find more information about our apps here: Log4Shell - bitvoodoo apps - 2021-12-13

As we cannot speak for other app vendors, we cannot be sure that other apps are safe. You might need to get in touch with other Atlassian Marketplace vendors. Should we get aware of a vulnerable app we will inform accordingly.

Please contact our support if you need assistance.

bitvoodoo Cloud

Your application is hosted with bitvoodoo

We have checked our installations according to the information in the FAQ. The installations have no configurations that could lead to misuse. As your Atlassian application uses the default configuration of Log4j, you applications are not affected by the exploit.

Apps

Third-party apps can still pose a risk. Atlassian is reviewing all apps and informs the vendors it the find a security risk. We have checked our bitvoodoo apps and found them to be risk-free. You can find more information about our apps here: Log4Shell - bitvoodoo apps - 2021-12-13

As we cannot speak for other app vendors, we cannot be sure that other apps are safe. You might need to get in touch with other Atlassian Marketplace vendors. Should we get aware of a vulnerable app we will inform accordingly.

Please contact our support if you need assistance.

Atlassian Cloud

Your application is with Atlassian Cloud

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

Further Recommendation

Please check all Java based software, beside Atlassian products, running in your organisation as this is a serious security risk.

Further Reading

- Original publication by LunaSec
- CVE-2021-44228
- Atlassian FAQ for CVE-2021-44228, CVE-2021-45046 and CVE-2021-45105

Support

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