Log4Shell - bitvoodoo apps - 2021-12-13

Contents

Date	13 Dec 2021
Product	• Apache Log4j 2
Vulnerability	Not applicable
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 - Products and hosting
Looking for information about Atlassian products and bitvoodoo hostings? Look here.

Dear customer,

On Thursday 9th December, developers and security researchers found a security vulnerability in Apache Log4j 2. Atlassian issued their own Security Advisory on 13th December.

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.

bitvoodoo apps

Data Center and Server

App	Status	Explanation
Paid Apps		
Viewtracker - Analytics for Confluence	NOT VULNERABLE	We do not use lookup and Confluence uses an old version of Log4j that is not affected.
Navitabs - Tabs for Confluence	NOT VULNERABLE	
Advanced Panelboxes for Confluence	NOT VULNERABLE	
Translations for Confluence	NOT VULNERABLE	
Chat for Confluence	NOT VULNERABLE	
Enterprise Theme for Confluence	NOT VULNERABLE	
Templates for Blog Posts for Confluence	NOT VULNERABLE	
Redirect for Confluence	NOT VULNERABLE	
Content Scheduler for Confluence	NOT VULNERABLE	
Advanced Search for Confluence	NOT VULNERABLE	

Attachment Tracking for Confluence	NOT VULNERABLE	
Search Analytics for Confluence	NOT VULNERABLE	
Custom Field Option Synchroniser	NOT VULNERABLE	Even though we use lookup of jndi for data sources, we use a static predefined prefix that contains "java:". This prevents other protocols from being used.
Free and Labs Apps		
Congrats for Confluence	NOT VULNERABLE	We do not use lookup and Confluence uses an old version of Log4j that is not affected.
Label Scheduler for Confluence	NOT VULNERABLE	
Macro Documentation for Confluence	NOT VULNERABLE	
SBB Widgets for Confluence	NOT VULNERABLE	
Viewtracker Supplier	NOT VULNERABLE	
Label Fixer	NOT VULNERABLE	

Cloud

App	Status	Explanation
Viewtracker - Analytics for Confluence	NOT VULNERABLE	Our Cloud apps are not affected. We do not use Log4j in our Cloud Apps. We work with the default logging of Spring Boot instead. See Log4J2 Vulnerability and Spring Boot
Navitabs - Tabs for Confluence	NOT VULNERABLE	
Advanced Panelboxes for Confluence	NOT VULNERABLE	
Translations for Confluence	NOT VULNERABLE	

What should I do?

Regarding our apps there is no need for action. If you are using the default configuration of Log4j or are on Atlassian Cloud, you are not affected (with the exception of Bitbucket). If you have ever customized the configuration of Log4j on your Atlassian on-premise installation to work with JMS Appenders, please disable them by following the mitigation described by Atlassian.

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.

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.
