Exécution du code à distance CVE-2021-44228 avec Apache Log4j

Background

On December 9, 2021, a newly discovered critical zero-day unauthenticated remote code execution (RCE) vulnerability (CVE-2021-44228, CVE-2021-4104) was reported in the open-source Java logging library Apache Log4j. Log4j is incorporated into many popular frameworks, making the impact widespread. It is easy to exploit and enables attackers to gain full control of affected servers.

Statement

WalkMe is aware of the vulnerability and has completed verification that this issue does not directly affect WalkMe products or services.

WalkMe is currently undertaking a comprehensive assessment to determine the potential indirect impact of the Log4j incident on internal and client information technology environments. This undertaking necessarily includes investigating any potential Log4j related risks or vulnerabilities of our sub contractors.

For all our applicable impacted in-house services, we have patched the log4j2 library and deployed the patched services into production.

Services that are running on the customer's client environment:

WalkMe Products	Status	Description
WalkMe Player	Not Impacted	Client side JS app. No Log4j directly/indirectly used.
WalkMe Editor	Not Impacted	Chromium based Electron. Client side JS app. No Log4j directly/indirectly used.
WalkMe Desktop	Not Impacted	Client side C# & Java app. No Log4j directly/indirectly used.
WalkMe Extension	Not Impacted	WalkMe browser extensions are JS apps. No Log4j directly/indirectly used.
WalkMe Mobile SDK	Not Impacted	WalkMe Mobile SDK for Android & iOS does not use Log4j.

Services that are managed and hosted by WalkMe:

WalkMe Products	Status	Description
WalkMe Insights	Not vulnerable	No direct vulnerable usage of Log4j.
WalkMe Mobile	Not vulnerable	The Log4j version used is not vulnerable.
WalkMe Platform	Not vulnerable	No direct vulnerable usage of Log4j.

We are working to identify applications and services reliant on Apache Log4j. These applications are being reviewed and upgraded if needed, to improve detection and mitigation of risks arising from the recent Log4j security issue.

We are performing a thorough scan of these services and hosts. Specifically, the exploit for CVE-2021-44228 relies on particular patterns in log messages and parameters, for example ${jndi:(ldap[s]?|rmi|dns):/[^n]+. For each potentially impacted service we perform a log analysis to expose any attempts at exploitation.

Impact

So far, we do not believe our products are vulnerable to exploitation, and are working closely with vendors across our supply-chain to ensure they complete investigations and mitigation as well.

Required Action

For WalkMe SaaS and WalkMe Self-hosted implementations, **no customer action is required**.

WalkMe is aware of the recommendations communicated by authorities and is continuing to monitor communications and assess if any critical recommendations impact any components of WalkMe's operations.

In general, WalkMe highly advises all customers who manage their own non-WalkMe related environments containing Log4j2 2.0 through 2.15 to update to Log4j-2.16.0 or later and contact their supply-chain vendors to ensure patching wherever applicable.

Update: December 17, 2021

Following our previous statement, we confirm that WalkMe is not impacted by the vulnerability CVE-2021-45046. ~~CVE-2021-45046 carries a lower CVSS score of 3.7 due to the impact of the condition that can be invoked.~~

For WalkMe SaaS and WalkMe Self-hosted implementations, **no customer action is required**.

WalkMe will continue to update as additional information becomes available. For any additional

details or assistance, please contact WalkMe Support.