13 December 2021

Enghouse Interactive has received information That a vulnerability in log4j has been discovered. This vulnerability is registered under CVE-2021-44228.

Description

The vulnerability impacts Apache-Log4j 2 versions 2.0 through to 2.14.1.

Risks and Exposure

Our analysis has shown that any Quality Management Suite installations that utilize the 3rd party full-text indexing service, Solr, are affected by this vulnerability. Installations that are not utilizing text (email, webchat) recording or transcription are not at risk because they do not utilize content indexing.

Recommendations and required actions

QMS	Impact	Recommendation	Required action
All versions	Solr server at risk	Follow recommendations on Solr website	See: https://solr.apache.org/security.html#apache-solr-affected-by-apache-log4j-cve-2021-44228