GeneXus™
Grow thru knowledge

セキュリティに関するお知らせ：

Apache Log4j を利用した

Java アプリケーションについて

2022 年 1 月 4 日

GeneXus Japan Inc.

本書には正確な情報を記載するように努めました。ただし、誤植や制作上の誤記がないことを保証するものではありません。なお、本書に記載されている画面はソフトウェアの更新などにより予告なく変更される場合があります。ご了承ください。

ジェネクサス・ジャパン株式会社

〒141-0031　東京都品川区西五反田 2 丁目 27 番 3 号

info@genexus.jp

http://www.genexus.jp

GeneXus™
Grow thru knowledge

目次

1. はじめに 4
2. GeneXus 社からのアナウンス 4
3. Log4j の更新対応について 5

1. はじめに

2021 年 12 月 10 日に「Apach log4j」に関する脆弱性（CVE-2021-44228）が公開されました。
該当のライブラリは GeneXus で利用しているため、GeneXus 社より下記の通りアナウンスが行われています。

2. GeneXus 社からのアナウンス

下記 URL にて GeneXus 社からのアナウンスが行われています。
https://www.genexus.com/en/news/read-news/important-security-notice-java-applications-with-apache-log4j
以下に日本語へ翻訳した内容を記載いたします。

重要なセキュリティに関するお知らせ：
Apache Log4j を使用した Java アプリケーションについて

Java アプリケーションで広く利用されている Apache Log4j ライブラリに関する重大なセキュリティリスクが確認され、報告が行われました。

Apache Log4j を利用した Java アプリケーションは、特定の状況下で、攻撃者がリモートでコードを実行できる可能性があります。
セキュリティレポート専用サイトや Log4j 自身のサイト内セキュリティセクションで詳細が説明されていますが、緊急の修正が非常に重要となります。

リスクを軽減するために、Apache Log4j による修正レポートに詳述される内容や GeneXus 社 SAC#50554 で報告された内容に従って、設定を行うことができます。

2021 年 12 月 16 日時点でも関係当局による分析が行われているため、GeneXus チームとしてもニュースを注視し、関連する措置を講じています。

SAC#50554 は、本事象および関連する問題を軽減または解決するために、関連情報を常に更新しています。

参照元：
CVE-2021-44228
CVE-2021-45046
Apache Log4j Security Vulnerabilities

---

3. Log4j の更新対応について

前述の Log4j の脆弱性発生を受け、GeneXus 社としてリリースしたアプリケーションへの都度対応ではなく、
GeneXus 自身の参照する Log4j を更新する対応方法についてアナウンスがありました。
この対応方法については下記日本語 SAC 内「回避策 1」として記載を行っていますので、
内容をご一読の上、ご対応をお願いいたします。
SAC#50554