App Bridge
Apache log4j2 脆弱性(CVE-2021-44228)の対応について

2021-12-14

平素より、当社 App Bridge をご利用いただき、誠に有難うございます。

2021 年 12 月に発表された Apache log4j2 脆弱性(CVE-2021-44228)の App Bridge における影響についてご報告致します。

１．影響範囲

App Bridge Ver.1.18.0 以降の Linux 系 Agent に Log4j（2.13.3）を使用しており、今回の脆弱性に該当します。対象となる Agent は、以下のとおりです。

・App Bridge Monitor Linux Agent Ver.1.18.0 以降
・App Bridge Kicker Linux Agent Ver.1.18.0 以降

※　Ver.1.18.0 未満では、Log4j 1 系バージョンを使用しており、本脆弱性の影響を受けません。

２．暫定対策

App Bridge は、Log4j による入力データ出力などを実施しないため、本脆弱性の影響は少ないと見ていますが、予期せぬ状況も考慮し、下記何れかの対策を推奨致します。なお、現在、Agent 起動スクリプトの変更パッチを準備中であり、準備出来次第ご連絡致します。

・Agent 起動スクリプトを変更し、起動オプションに-Dlog4j2.formatMsgNoLookups=true を追加する
・環境変数に LOG4J_FORMAT_MSG_NO_LOOKUPS="true"を設定する

３．本対策

次バージョン以降の Linux Agent では、対策版 Log4j（2.15.0 以降）を使用します。次バージョンのリリースは 2022 年 1 月を予定しています。

４．本件に関するお問合せ先

株式会社日立システムズ　App Bridge サポート窓口
mailto:info@app-bridge.com

以上