2021 年 12 月 17 日

ODIP をご導入のお客様へ

株式会社インテリジェント・モデル
品質管理部

Apache Log4j の脆弱性(CVE-2021-44228)に関する ODIP 製品への影響について

平素より格別のご高配を賜り厚く御礼申し上げます。

先般、独立行政法人情報処理推進機構（IPA）[i] から、Apache Log4j[ii] に重大な脆弱性があり、その脆弱性を悪用したと思われる攻撃が国内で観測されたとの注意喚起がありました。この脆弱性によって弊社が提供する ODIP 製品が受ける影響及び対策についてご案内いたします。

記

1. 脆弱性の概要

Apache Log4j は、Apache Software Foundation がオープンソースで提供している Java ベースのロギングライブラリです。この Apache Log4j において、遠隔の第三者が細工したデータを送る事で、任意のコマンドを実行される可能性があります。

CVE-2021-44228 として登録されたこの脆弱性は、CVSS スコアに 10.0（最も深刻なリスク数値）が付けられています。

2. ODIP 製品における Apache Log4j の使用状況及び脆弱性による影響

v4.1 より前の ODIP 製品では、Apache Log4j 1.2.14 のライブラリを使用しています。このライブラリは、本脆弱性の対象ではありません。

v4.1 以降の ODIP 製品では、Apache Log4j 2.11.2 のライブラリを使用しています。このライブラリは本脆弱性の対象であり、脆弱性が悪用される可能性があります。ただし、ODIP 製品は、その性質上バッチサーバなど外部ネットワークから隔離された環境で稼働することが多く、遠隔操作によって本脆弱性の影響を受ける可能性は低いと考えられます。

3. ODIP 製品としての対策

v4.0 以前の ODIP 製品をご利用中の場合は、特に対策を行っていただく必要はございません。**v4.1 以降の ODIP 製品をご利用中の場合は、ODIP 製品内にバンドルされている Apache Log4j のライブラリを、本脆弱性対策後の最新版（Apache Log4j 2.16.0）にアップデートすることで本脆弱性による影響を回避することができます。**

v4.1 以降の ODIP 製品では、Apache Log4j の最新版へのアップグレードによる無影響確認を完了しており、必要に応じて Log4j の最新版ライブラリを提供する用意ができております。

当該バージョンの ODIP 製品をご利用中のお客様におかれましては、適用要否をご判断いただきまして、弊社までご連絡をいただければと存じます。

4. お問い合わせ先

電話番号： 03-5531-0062（受付時間（月～金）9:30～17:30））

メールアドレス： info@imkk.jp

以 上

---

[i] 独立行政法人情報処理推進機構（IPA）
https://www.ipa.go.jp/security/ciadr/vul/alert20211213.html

[ii] Apache Log4j
https://logging.apache.org/log4j/2.x/