2021年12月13日
（更新日：2021年12月17日）

お客様各位

株式会社セゾン情報システムズ
カスタマーサービスセンター
HULFTテクニカルサポートセンター

Apache Log4jの脆弱性による弊社製品への影響について

拝啓

平素より、テクニカルサポートサービスをご利用いただき、誠にありがとうございます。

2021 年 12 月 10 日に公開された Apache Log4j の脆弱性（CVE-2021-44228）による HULFT 及び関連製品の影響と対応方針についてご報告をさせていただきます。

敬具

-記-

各製品については、最新バージョンの対応について記載をさせていただいております。

また現在調査中の製品につきましては、調査完了後に本文書を更新することでの告知とさせていただきます。

■HULFT

本脆弱性の発生要因となるモジュールは使用されていないため、影響はありません。

■HULFT　Script

本脆弱性の発生要因となるモジュールは使用されていないため、影響はありません。

■HULFT-WebFileTransfer

Ver.3.1.0A 以下の製品については、本脆弱性の発生要因となるモジュールは使用されていないため、影響はありません。

Ver.3.1.1～Ver.3.2.1 については、log4j2(2.11.1)を組み込んでいますが、(別紙)記載の通り、調査結果として影響が無いことを確認しています。

■HDC-EDI Base/HDC-EDI Manager

本脆弱性の発生要因となるモジュールは使用されていないため、影響はありません。

■iDIVO

本脆弱性の発生要因となるモジュールは使用されていないため、影響はありません。

■HULFT-WebConnect

本脆弱性の発生要因となるモジュールは使用されていないため、影響はありません。

■HULFT IoT

本脆弱性の発生要因となるモジュールは使用されていないため、影響はありません。

■DataMagic

本脆弱性の発生要因となるモジュールは使用されていないため、影響はありません。

■SIGNAlert

本脆弱性の発生要因となるモジュールは使用されていないため、影響はありません。

■HULFT-HUB

本脆弱性の発生要因となるモジュールは使用されていないため、影響はありません。

■DataSpider Servista、DataSpider Servista with Software Protection

本脆弱性の発生要因となるモジュールは使用されていないため、影響はありません。

■DataSpider Cloud

本脆弱性の発生要因となるモジュールは使用されていないため、影響はありません。

■PIMSYNC

本脆弱性の発生要因となるモジュールは使用されていないため、影響はありません。

■DataSpider BPM

本脆弱性の発生要因となるモジュールは使用されていないため、影響はありません。

■Thunderbus

本脆弱性の発生要因となるモジュールは使用されていないため、影響はありません。

■HULFT DataCatalog

本脆弱性の発生要因となるモジュールは使用されていないため、影響はありません。

※備考

[該当の脆弱性情報]
JPCERT/CC
Apache Log4j の任意のコード実行の脆弱性（CVE-2021-44228）に関する注意喚起
https://www.jpcert.or.jp/at/2021/at210050.html

【改訂履歴】

2021年12月13日	初版作成
2021年12月13日	調査完了製品を更新
2021年12月14日	調査完了製品を更新
2021年12月15日	調査完了製品を更新、調査完了予定を追記
2021年12月17日	調査完了製品を更新、調査結果詳細を(別紙)として追加

以上

(別紙)HULFT-WebFileTransfer Ver.3.1.1～Ver.3.2.1 影響調査結果について

HULFT-WebFileTrasfer Ver.3.1.1～Ver3.2.1 について、脆弱性の影響を受けないことを確認いたしました。
弊社側で調査した内容を以下に記載します。

―調査結果―

Ver.3.1.1～Ver.3.2.1 は log4j のモジュールとして log4j2(V2.11.1)と log4j(V1.2.17)の両方を組み込み使用しています。
HULFT-WebFileTrasfer が内部的に使用している struts のログ出力で log4j2(V2.11.1)を呼び出していますが、log4j-to-slf4j というライブラリを使用し、実際のログ出力処理は log4j(V1.2.17)が実施します。
このため、ログ出力処理自体において log4j2(V2.11.1)を利用していない事となります。

さらに、今回の脆弱性の条件である、log4j2 の lookup 機能が動作するかどうかを、以下 2 点の観点で調査いたしましたが、lookup 機能は動作しませんでした。

・製品ソースコード調査
・動作試験

以上