【Webセキュリティ企業による緊急公開資料】

情シス・IT管理者、そしてITに関わるすべての方へ！

Apache Log4j

脆弱性の影響緩和のために 今できること

【資料緊急公開！】

公開日：2021/12/14

株式会社セキュアスカイ・テクノロジー

はじめに

2021年12月9日より世界的に報告され始めたApache Log4j の任意のコード実行の脆弱性[CVE-2021-44228]の危険性および緊急性を踏まえ、被害を受ける可能性を感じているが情報収集や対策を早急に行う必要に迫られている情報システム部門・IT管理者と、ITに関わるすべての方に向けて、本脆弱性の注意喚起と影響緩和を目的とした『Apache Log4jの影響緩和のために今できること』を緊急公開いたしました。

本資料は、現時点で考えられる対応について、まとめたものであり、「これだけやれば大丈夫」ということではなく、「今できること」をお伝えするものです。

現在進行形で状況が変化しているため、各ベンダーやJPCERT/CCとIPAなど信頼できる情報源の最新情報を随時確認してください。

アジェンダ

- 今、何が起きているのか
- 「Apache Log4j」の脆弱性による影響の大きさ
- 影響を受ける範囲は？
- 被害を受けたらどうなるの？
- 情シス・IT管理者が今できること [その1]〜[その3]
- ITに関わるすべての方（個人）が今できること
- 大事なお願い

今、何が起きているのか

- 2021年12月10日、Javaを利用したシステムで広く利用されているログ記録用のライブラリ「Apache Log4j」に非常に危険度の高い脆弱性があることが判明*し大きな問題になっている
- Javaは幅広いシステムやサービス、製品で利用されており、世界中のITインフラに影響が及んでいるため、インターネットを利用するすべての方に関わる影響範囲の大きい出来事が現在進行中で進んでいる

* 参照元（JPCERT/CC）：https://www.jpcert.or.jp/at/2021/at210050.html

「Apache Log4j」の脆弱性による影響の大きさ

- 脆弱性の深刻度は、CVSS*1スコア基準値で最大の「10.0」緊急（Critical）
- 特別なスキルを持たない攻撃者でも容易に攻撃がおこなえる
- 対象となるシステムが多岐にわたる
- 攻撃後に自由に悪用できる
- すでに国内企業において、被害*2が確認されている
- 企業規模に関係なく被害に遭う可能性がある
- 今後もより広い範囲で影響が出ることが予想される

*1 参照元（IPA）：https://www.ipa.go.jp/security/vuln/CVSS.html

*2 参照元（IPA）：https://www.ipa.go.jp/security/ciadr/vul/alert20211213.html

影響を受ける範囲は？

- Javaで開発されている非常に多くのシステム・ソフトウェア*
  - JPCERT/CCとIPAの最新情報を随時チェックしよう
- サーバー側だけでなく、企業内のPCや個人のPCで利用するソフトウェア
- 公開されているサーバーだけではなく、ログや通信内容を介して内部ネットワーク上のサーバーや機器も波及的に影響が広がる可能性がある

例）
- Webサイト/Webサービス/Webシステム
- オンプレミスやクラウド環境などサーバーサイド
- 企業内のログ監視システム、ネットワーク機器
- インフラ、企業内の基幹システムやPC
- IoT機器や家庭内のPC

* 影響受ける製品に関する参考ページ（BlueTeam CheatSheet * Log4Shell*）
：https://gist.github.com/SwitHak/b66db3a06c2955a9cb71a8718970c592

被害を受けたらどうなるの？

- **任意コード実行が可能なため、**あらゆる攻撃がおこなえる
- 該当コンピュータの乗っ取り、マルウェア配布、情報漏えい、仮想通貨マイニングなど、あらゆる脅威の可能性がある
- 取引先への詐欺メールの送信や、ランサムウェアによる社内情報資産の暗号化など、**事業継続への大きな被害**もあり得る
- 自社への被害により**取引先にも影響をあたえる**可能性がある

情シス・IT管理者が今できること [その1]

Apache Log4jがどこで使われているかの判断は難しいため、社内のシステムやソフトウェア、機器のリリース情報を確認し、以下についてベンダーや開発者に確認する

- ✔ 本脆弱性の影響を受けるか
- ✔ 対策されたバージョンが提供されているか
- ✔ 対応方法がない場合の回避方法

脆弱性のあるバージョンを使っていた場合は、すでに攻撃されていることを前提に調査を開始する

- ✔ ログファイルに痕跡が残っていないか
- ✔ 不審なファイルやプロセスが動いていないか、不審な通信が発生していないか

利用しているクラウドサービスの公式情報、サポート情報を確認する

- ✔ 本脆弱性の影響を受けるか
- ✔ 影響受ける場合の対応方法

情シス・IT管理者が今できること [その2]

- **社内への注意喚起**
  - 全員に関係する重大な脆弱性であることを改めて周知
  - 社内で利用中のソフトウェア・クラウドサービスの確認
    - 提供元からの情報収集と対策
    - 収集した情報の集約依頼
  - 改めて不審な受信メールやリンクへの注意喚起
  - 被害の可能性に気づいたときの連絡体制の確認

情シス・IT管理者が今できること [その3]

- **取引先への協力依頼内容**
  - 現時点での自社の対応状況の共有
  - 今後新たな情報が出てきた場合の共有方法のお知らせ
  - 本脆弱性に関して取引先内で影響があった場合の情報提供依頼
  - 自社ならびに取引先の双方で影響があった場合の対応方法共有（システム停止等の可能性について事前共有）

ITに関わるすべての方（個人）が今できること

- 不審なメールやリンクをむやみにクリックしない
  - 知人からのメールであっても、いつも以上の注意が必要！
- ご自身のPCで利用しているソフトウェアを更新する
- 本脆弱性は広範囲に影響が出る可能性があるため、あらゆる攻撃に対して、いつも以上に注意を払う必要がある

大事なお願い

本脆弱性の影響範囲は広く、どこまでの影響があるか正確な判断が難しい状態です。

本資料は、現時点で考えられる対応について、まとめたものであり、「これだけやれば大丈夫」ということではなく、「今できること」をお伝えするものです。

現在進行形で状況が変化しているため、各ベンダーやJPCERT/CCとIPAなど信頼できる情報源の最新情報を随時確認してください。

最後に、本脆弱性による被害拡大防止と影響緩和の一助となりますようご活用ください。あわせて、本資料を必要とするより多くの方へお伝えいただけると幸いです。

本資料提供元

「インターネットを安全にしたい」という想いを原点に、SSTは2006年に設立された
Webアプリケーションセキュリティの専門企業です。

社名	株式会社セキュアスカイ・テクノロジー　[SST]
設立	2006年
事業	Webアプリケーションに特化したセキュリティサービス クラウド型WAFサービス「Scutum」、脆弱性診断サービス、セキュリティ教育・支援サービス、セキュリティコンサルティング、その他
代表取締役	大木 元（OOKI Hajime）
本社所在地	東京都千代田区神田司町2-8-1 PMO神田司町2F
福岡ラボ	福岡県福岡市中央区天神1-9-17 福岡天神フコク生命ビル14F
URL	https://www.securesky-tech.com/