2022 年 05 月 25 日

サービス＆セキュリティ株式会社 e-Gate センター

Spring Framework と Spring Cloud Function の脆弱性について

1. 概要

2022 年 3 月末に相次いで、Java アプリケーションフレームワーク「Spring」に関連する脆弱性が公開されました。

情報の公開から 1 か月以上経過した現在でもこの脆弱性を悪用するサイバー攻撃は依然として続いており、e-Gate センターでも本脆弱性を悪用した攻撃を観測しております。

今回はこの脆弱性の詳細、攻撃手法と最新の動向について紹介いたします。

2. 脅威の詳細

2022 年 3 月 29 日から 3 月 31 日に相次いで、オープンソースの Java アプリケーションフレームワークである「Spring」の異なるコンポーネントに存在する 2 つの重大な脆弱性（CVE-2022-22963 および CVE-2022-22965）が公開されました。どちらの脆弱性も、攻撃者が特定の HTTP リクエストを介して、リモートでコードを実行する可能性があり、CVSSv3（※1）は 10 点満点中 9.8 点と評価されています。これらの脆弱性は、サーバ上の幅広いサービスやアプリケーションに影響するため、迅速な対策が必要となります。当脆弱性はすでに修正バージョンが更改されているため、影響を受けるユーザーは迅速にアップグレードする必要があります。詳細については以下に記載する表 1 をご覧ください。

また、この 2 つの脆弱性は異なるコンポーネントに対するそれぞれ異なる脆弱性である点にご注意ください。

(1) CVE-2022-22963

「Spring」のサーバレス実行環境である「Spring Cloud Function」における脆弱性で、SpEL 脆弱性とも呼ばれます。ルーティング機能を有効にしている場合に、リモートの攻撃者が特定の細工した「SpEL（Spring Expression Language）」を使用してサーバ上でコードを実行することができます。攻撃が成功するとローカル環境にあるリソースへアクセスされるおそれがあります。

(2) CVE-2022-22965

「Spring」の主要なコンポーネントの 1 つでフレームワークの中核となる「Spring Core」における脆弱性で、SpringShell または Apache Log4j の脆弱性にちなんで Spring4shell とも呼ばれます。JDK 9（Java 9）以降で実行されている Spring MVC または Spring WebFlux アプリケーションに影響があり、リモートの攻撃者がデータバインディング（※2）を介してコードを実行することができます。攻撃が成功すると侵害されたサーバにウェブシェル（※3）がインストールされ、さらにコマンド実行されるおそれがあります。

CVE番号	**CVE-2022-22963**	**CVE-2022-22965**
CVSSv3	9.8	9.8
脆弱性対象	Spring Cloud Function	Spring Framework
脆弱性対象バージョン	Spring Cloud Function -3.1.6 -3.2.2 -およびそれ以前の古いバージョン	**次の条件が全て成立する場合** ・JDK 9以上 ・サーブレットコンテナとしてのApache Tomcat ・WARファイルとしてのパッケージ化 ・spring-webmvc または spring-webflux との依存関係 ・Spring Framework -5.3.0 から 5.3.17 -5.2.0 から 5.2.19 -およびそれ以前の古いバージョン
対策	Spring Cloud Function 3.1.7に更新 Spring Cloud Function 3.2.3に更新	Spring Framework 5.3 5.3.18以上に更新 Spring Framework 5.2 5.2.20以上に更新 Spring Bootを利用している場合はSpring Framework 5.3.18に依存しているため脆弱性対応のバージョンに更新する。 Spring Boot 2.6 2.6.6以上に更新 Spring Boot 2.5 2.5.12以上に更新 Tomcat 9.0.62以上に更新

【表 1】Spring に見つかった 2 つの脆弱性

2021 年末に発生し注目を集めたオープンソースの Apache Log4j の脆弱性問題につづき、同じくオープンソースのフレームワークである「Spring」に危険度の高い脆弱性が報告されました。オープンソースソフトウェア（以降は OSS と記載）は、開発スピード向上などの目的で広く活用されており、日々使用しているソフトウェアのあらゆる部分に密接に組み込まれているためセキュリティ対策が不可欠です。

システムで利用している OSS を把握し、脆弱性情報が公開されていないか常に最新の情報に注視する必要があります。

特に利用している OS のバージョンを正しく管理し、脆弱性が発覚した場合は適宜バージョンアップを行うなど迅速な対応が求められます。

※1:CVSSv3 とは、共通脆弱性評価システムといい、基本評価基準・現状評価基準・環境評価基準の 3 つの基準で IT 製品のセキュリティ脆弱性の深刻さを評価した値です。情報システムの脆弱性に対するオープンで汎用的な評価手法で、0.0～10.0 の範囲（値が大きいほど深刻）で深刻度をスコア化しています。

※2:データバインディングとは、アプリケーションのユーザインタフェースと、データソースとの間の接続を確立する処理のことです。データが変更されると自動的に「バインド」されているもう一方にも反映されます。

※3:ウェブシェルとは、Web サーバに対して任意のコマンドの実行を可能にするバックドアの 1 種です。攻撃者は対象のサーバにウェブシェルをインストールすることにより、サーバを遠隔で操作することができます。

3. 最新動向

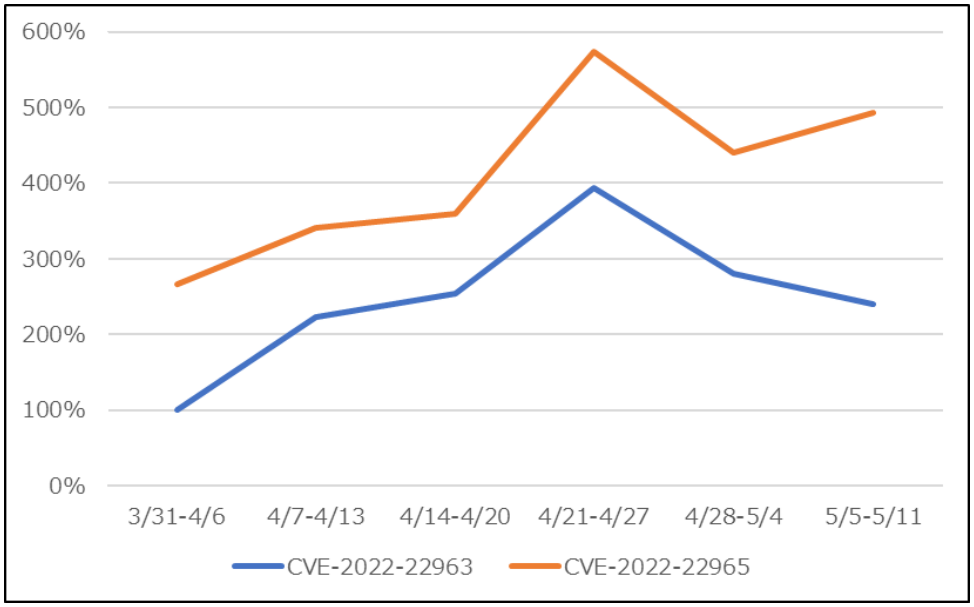
本脆弱性が公開されて以降、悪用を試みる攻撃が多数報告されています。中でも、CVE-2022-22965 の脆弱性を悪用する攻撃の試行が活発となっています。

トレンドマイクロは、本脆弱性を悪用してサーバに「Mirai」を感染させる攻撃がみられたと報告しています。「Mirai」は 2016 年以来長く続いている脅威で、Web カメラやルーターなどの IoT 機器を標的とするマルウェアです。感染した IoT 機器を使って巨大な「ボットネット」を形成しそのボットネットに指示を出すことで DDoS 攻撃を行います。

また、同脆弱性を悪用し、仮想通貨をマイニングするマルウェア「コインマイナー」に感染させる攻撃事例も確認されています。コインマイナーに感染するとマイニング処理のために CPU などのリソースを使われてしまうため端末の処理能力が低下し、過負荷によりシャットダウンしてしまうケースもあります。

4. e-Gate センターにおける攻撃検知の推移

e-Gate センターでは「Spring」の脆弱性をついた攻撃を観測しております。脆弱性が公開されてから 4 月 27 日にかけての大幅な増加は収束していますが、特に CVE-2022-22965 に関連するイベントに関しては依然として高い検知量を維持しています。前述の通り、この脆弱性を悪用しマルウェアへの感染を試みる攻撃も報告されており、今後しばらくは高水準の検知量が継続すると予想されるため警戒が必要です。実際の推移観測結果が図 1 となります。



【図 1】e-Gate センターにおける攻撃イベント数の推移

(3/31-4/6 の期間の「CVE-2022-22963」に関連するイベント検知数を 100%として算出)

5. 参考情報

・ TrendMicro

Spring4Shell（CVE-2022-22965）を悪用したボットネット「Mirai」の攻撃を観測

https://blog.trendmicro.co.jp/archives/31044

Spring4Shell（CVE-2022-22965）を悪用したコインマイナーの攻撃を観測

https://blog.trendmicro.co.jp/archives/31203

・ VMware

CVE-2022-22963: Remote code execution in Spring Cloud Function by malicious Spring Expression
https://tanzu.vmware.com/security/cve-2022-22963
Spring Framework RCE, Early Announcement
https://spring.io/blog/2022/03/31/spring-framework-rce-early-announcement

6. e-Gate の監視サービスについて

e-Gate のセキュリティ機器運用監視サービスでは、24 時間 365 日、リアルタイムでセキュリティログの有人監視を行っております。サイバー攻撃への対策としてセキュリティ機器を導入する場合、それらの機器の運用監視を行い、通信が攻撃かどうかの分析、判断をして、セキュリティインシデント発生時に適切に対処できるようにすることが重要です。e-Gate のセキュリティ監視サービスをご活用いただきますと、迅速なセキュリティインシデント対応が可能となります。

また、e-Gate の脆弱性診断サービスでは、お客様のシステムにて潜在する脆弱性を診断し、検出されたリスクへの対策をご提案させていただいております。

監視サービスや脆弱性診断サービスをご活用いただきますと、セキュリティインシデントの発生を予防、また発生時にも迅速な対処が可能なため、対策コストや被害を抑えることができます。

■総合セキュリティサービス e-Gate

SSK（サービス＆セキュリティ株式会社）が 40 年以上に渡って築き上げてきた「IT 運用のノウハウ」と最新のメソッドで構築した「次世代 SOC“e-Gate センター”」。この 2 つを融合させることによりお客様の情報セキュリティ全体をトータルにサポートするのが SSK の“e-Gate”サービスです。e-Gate センターを核として人材・運用監視・対策支援という 3 つのサービスを軸に全方位のセキュリティサービスを展開しています。

【参考 URL】
https://www.ssk-kan.co.jp/e-gate/

※本資料には弊社が管理しない第三者サイトへのリンクが含まれています。各サイトの掲げる使用条件に従ってご利用ください。
　リンク先のコンテンツは予告なく、変更、削除される場合があります。
※掲載した会社名、システム名、製品名は一般に各社の登録商標 または商標です。

«お問合せ先»
サービス＆セキュリティ株式会社
〒150-0011
東京都渋谷区東 3 丁目 14 番 15 号 MO ビル 2F
TEL 03-3499-2077
FAX 03-5464-9977
sales@ssk-kan.co.jp