2021 年 02 月 24 日

サービス＆セキュリティ株式会社 e-Gate センター

注意喚起：Apache 製ソフトウェアの脆弱性を突いた攻撃について

1. 概要

Apache Software Foundation は、「Apache HTTP Server」を始めとした Web サーバを運用する上で欠かせないソフトウェアを数多く提供しています。

その一方で、Apache 関連のソフトウェアの脆弱性が多数発見されており、国内でも IPA（情報処理推進機構）や JPCERT コーディネーションセンターからたびたび注意喚起が行われています。「脆弱性対策情報の公開に伴う悪用増加」は IPA が毎年発表している「情報セキュリティ 10 大脅威」でも 2020 年の 14 位から 2021 年は 10 位に上昇しており、注意が必要な脅威の 1 つです。

2021 年 1 月には早くも JPCERT より「Apache Tomcat」の脆弱性に関する注意喚起が行われています。また、2020 年末以降、e-Gate センターでも Apache 関連のソフトウェアの脆弱性を狙った攻撃の増加を検知しております。

今回はそれらの脆弱性の詳細と対策についてご紹介いたします。

2. Apache のシェアと利用のリスクについて

Apache Software Foundation が提供するソフトウェアは無償で利用可能なオープンソースソフトウェア（OSS）であり、その長い歴史から信頼性も高く、また稼働する OS を問わない利便性が特徴です。このことから Apache 関連のソフトウェアは世界中で利用されており、実際に Apache HTTP Server は Netcraft の調査によれば 2021 年 1 月時点で世界における Web サーバの約 1/4 を占めています。その高いシェアゆえに悪意ある攻撃者のターゲットとなりやすいソフトウェアであるとも言えます。

Apache 関連ソフトウェアの脆弱性の過去事例としては、2020 年に「Apache Tomcat」（以下 Tomcat）の脆弱性・通称「Ghostcat」(CVE-2020-1938) が明らかとなっており、多数の PoC コード（実証コード）が公開され、容易に攻撃可能な状況となったことから問題となっています。

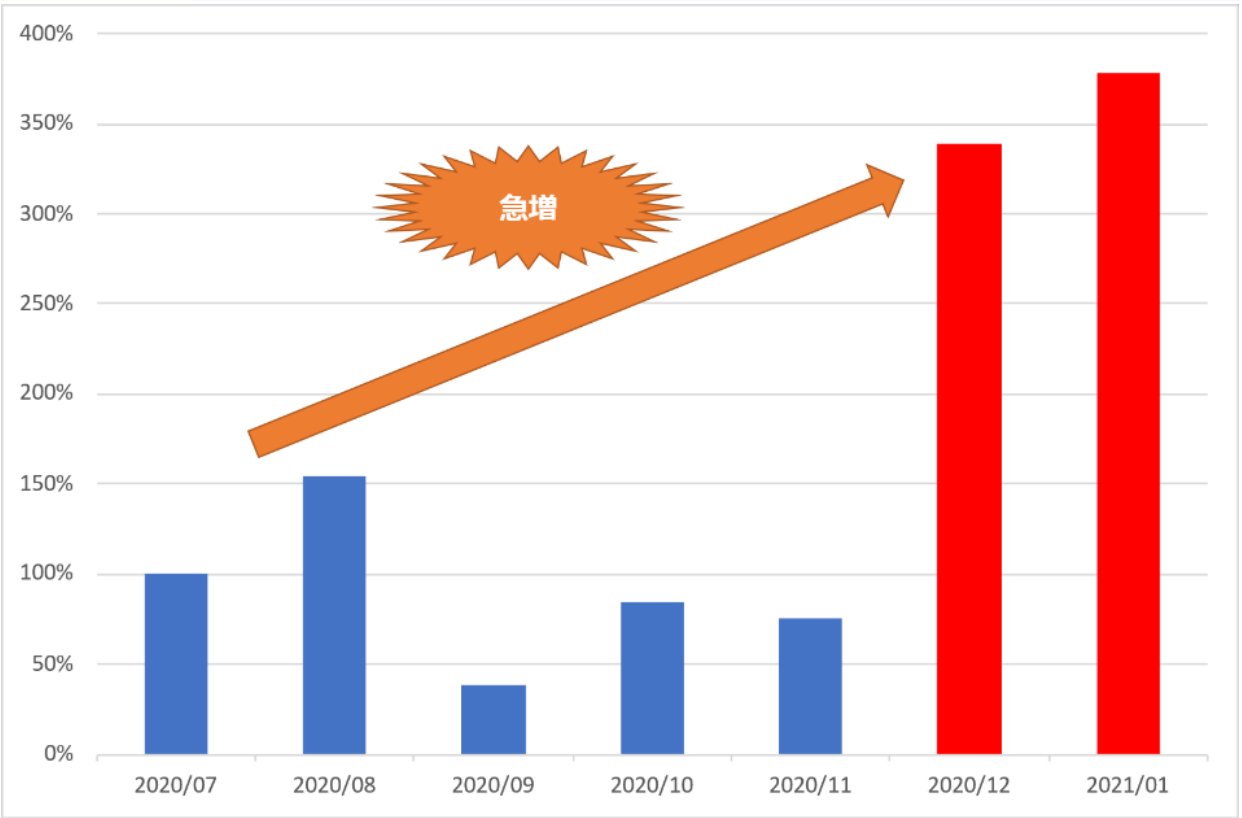
また、Java の Web アプリケーションを作成するためのフレームワーク「Apache Struts 2」（以下 Struts2）の脆弱性について、過去に弊社の e-Gate セキュリティニュースで取り上げております。詳細は下記ニュースをご参照ください。

https://www.ssk-kan.co.jp/topics/topics_cat05/?p=9257

3. e-Gate センターにおける Apache 関連の攻撃イベントの傾向

e-Gate センターでは Apache 関連ソフトウェアの脆弱性をついた攻撃の増加を観測しております。特に 2020 年 12 月以降においてその数は前月の 4 倍以上まで急増しており、今後も攻撃の増加が予想されます。

攻撃の傾向としては、先に挙げた Tomcat や Struts2 に加え、「Apache Solr」（以下 Solr）の脆弱性を狙った攻撃が多数を占めております。



【図 1】e-Gate センターにおける Apache 関連の攻撃イベント数の推移（2020 年 7 月を 100%として算出）

4. 「Apache Tomcat」脆弱性（CVE-2021-24122）の詳細

Tomcat は Java Servlet や JavaServer Pages（JSP）を実行するための Web コンテナ（サーブレットコンテナ）です。

Apache HTTP Server が Web サーバとしてテキストや画像などの静的なコンテンツを提供するのに対し、Tomcat は Web サーバ上で Java スクリプトを動作させるために必要な環境を提供し、動的なコンテンツを提供します。Tomcat 自体にも Web サーバの機能が存在しますが、別の Web サーバと連携させることによりサーブレットコンテナとしての用途に特化させることができます。

2021 年 1 月 15 日に JPCERT より Tomcat の脆弱性（CVE-2021-24122）について注意喚起が行われています。

当該脆弱性は NTFS（Windows 系のファイルシステム）を利用してネットワーク上からリソースを提供する場合に発生します。Java API の File.getCanonicalPath()の予期しない動作によってセキュリティの制約回避や JSP のソースコードの漏洩が発生する可能性があります。

対象システムは下記のバージョンです。

- Apache Tomcat 10.0.0-M1 から 10.0.0-M9
- Apache Tomcat 9.0.0.M1 から 9.0.39
- Apache Tomcat 8.5.0 から 8.5.59
- Apache Tomcat 7.0.0 から 7.0.106

5. 「Apache Solr」脆弱性（CVE-2018-1308）の詳細

Solr は全文検索エンジンです。

2018 年に Solr の XML 外部実体攻撃（XXE 攻撃）に対する脆弱性（CVE-2018-1308）の情報が公開されていますが、e-Gate センターにおいて検知数が急増している攻撃の 1 つにその脆弱性を突いた攻撃が挙げられます。

XXE 攻撃は特殊な XML 入力を送信することで、任意のローカルファイルの参照や内部ネットワークへのリクエストが可能になる攻撃手法です。

対象システムは下記のバージョンです。

- Apache Solr 1.2 から 6.6.2
- Apache Solr 7.0.0 から 7.2.1

6. 対策

・最新アップデートの適用

開発元より公開されている脆弱性を修正したバージョンへのアップデートが推奨されます。

CVE-2021-24122 については、下記のバージョンで当該脆弱性が修正されています。

- Apache Tomcat 10.0.0-M10 以降
- Apache Tomcat 9.0.40 以降
- Apache Tomcat 8.5.60 以降
- Apache Tomcat 7.0.107 以降

CVE-2018-1308 については、下記のバージョンで当該脆弱性が修正されています。

- Apache Solr 6.6.3 以降
- Apache Solr 7.3.0 以降

・セキュリティ機器による攻撃通信の監視

Firewall や IPS（侵入防御システム）等のセキュリティ機器により、不審な通信を検知・遮断することも一定の効果が見込めます。

7. 参考

・Netcraft

January 2021 Web Server Survey

https://news.netcraft.com/archives/2021/01/28/january-2021-web-server-survey.html

・IPA

情報セキュリティ 10 大脅威 2021

https://www.ipa.go.jp/security/vuln/10threats2021.html

Apache Tomcat における脆弱性（CVE-2020-1938）について

https://www.ipa.go.jp/security/ciadr/vul/alert20200225.html

・JPCERT/CC
Apache Tomcat の脆弱性（CVE-2021-24122）に関する注意喚起
https://www.jpcert.or.jp/at/2021/at210002.html

・JVN
Apache Tomcat における Java API の実装不備に起因する情報漏えいの脆弱性
https://jvn.jp/vu/JVNVU96136392/
Apache Solr における XML 外部エンティティの脆弱性
https://jvndb.jvn.jp/ja/contents/2018/JVNDB-2018-004003.html

8. 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