2021 年 11 月 29 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 HTTP Server のパストラバーサルの脆弱性をついた攻撃について

1. 概要

2021 年 10 月 6 日に The Apache Software Foundation より Apache HTTP Server のバージョン 2.4.49 にパストラバーサルの脆弱性が存在することが発表されました。（CVE-2021-41773）

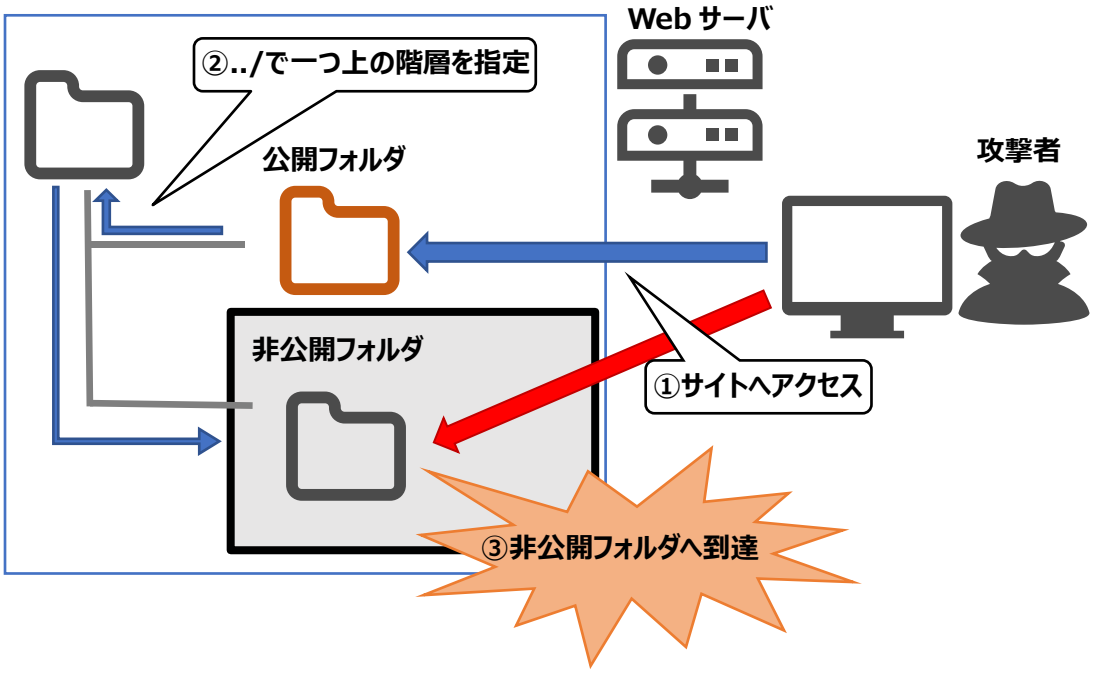
本脆弱性の修正としてバージョン 2.4.50 が提供されましたが、別のパストラバーサルの脆弱性（CVE-2021-42013）があることが判明し、修正バージョン 2.4.51 がリリースされました。

今回はこの脆弱性の詳細とパストラバーサル攻撃の手法、対策について紹介いたします。

2. パストラバーサルの攻撃の詳細

パストラバーサル(別名：ディレクトリトラバーサル)とは Web サーバ上のアクセスが許可されていない非公開のファイルにアクセスする攻撃です。Web ページは HTML ファイル等のパスを URL の中で指定し、表示します。このときカレントディレクトリからアクセスを許可していないディレクトリを URL の中で指定することで攻撃を試みます。

攻撃の一例として、現在アクセスしているカレントディレクトリから一つ上の階層を表す「../」を指定し、次にアクセスの許可されていない非公開フォルダへの移動を指定した場合、脆弱性のあるシステムを使用しているとファイルにアクセスされてしまう危険性があります。



【図 1】パストラバーサル攻撃の一例

3. 攻撃による被害

攻撃が成功した場合、いくつかの被害が考えられます。

●情報漏えい

非公開のファイルが攻撃者に参照されるので、Web サーバ上に個人情報など機密情報がある場合、その情報漏えいの危険性があります。

●データの改ざん

非公開のファイルに不正にアクセスし、データを改ざんされる恐れがあります。公開している自社の Web ページの改ざんや、システムの運用に必要なデータが改ざんされることにより、サービスの停止などの危険性があります。

●アカウントの乗っ取り

パストラバーサルの攻撃によりアカウントを管理しているフォルダへアクセスされた場合、ログイン情報を用いてシステムの乗っ取りが行われる可能性があります。

4. Apache について

Apache HTTP Server は世界中で広く使われている Web サーバ・ソフトウェアです。

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、提供の Apache HTTP Server についても同様です。Netcraft の調査によると 2021 年 10 月時点で世界における Web サイトの約 1/4 で使用されており、その高いシェアから攻撃者の標的になりやすいと考えられます。

Apache を始めとした OSS の魅力は無償で利用可能であるので開発・運用におけるコストの削減が期待できることです。一方でオープンソースであることから、何らかのアクシデントが起きた際、補償やサポートなどを受けることができないことを留意しておく必要があります。

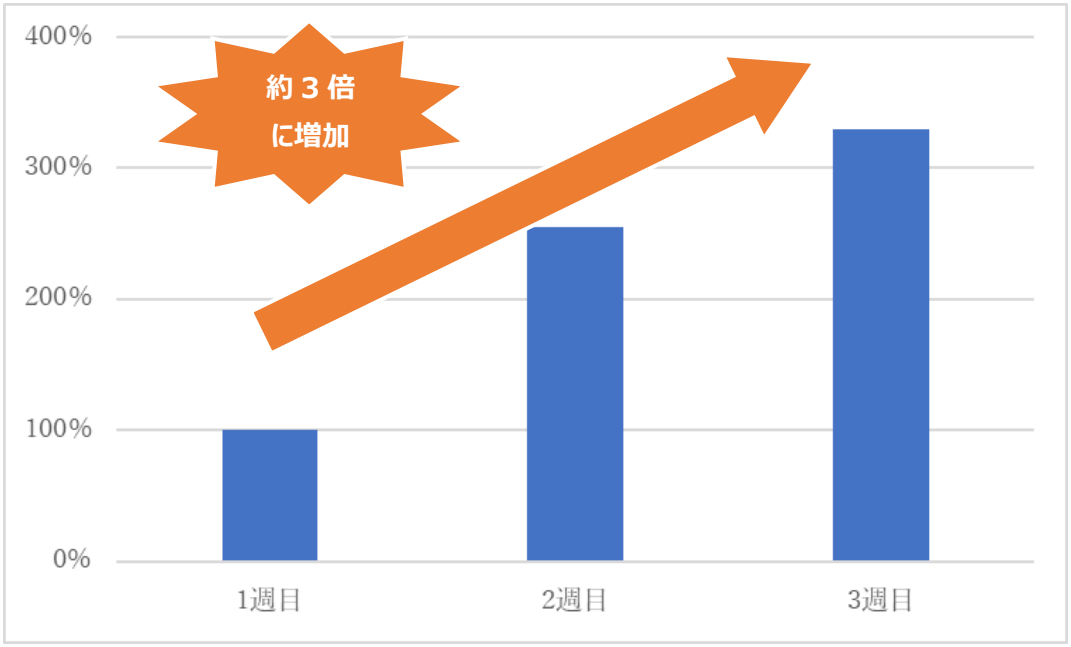
Apache の脆弱性をついた攻撃については過去に弊社の e-Gate セキュリティニュースで取り上げております。詳細は下記ニュースをご参照ください。

https://www.ssk-kan.co.jp/topics/topics_cat05/?p=11458

5. 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 Apache HTTP Server のパストラバーサルの脆弱性をついた攻撃を継続的に検知しています。

下図は本脆弱性が発表されて以降、一週ごとの検知数です。



【図 2】e-Gate センターにおける CVE-2021-41773, CVE-2021-42013 の検知

本脆弱性に対する攻撃は発表されて以降増加傾向にあり、引き続き注意が必要です。

6. 攻撃対策

The Apache Software Foundation より本脆弱性を悪用する攻撃を検知していることが発表されており、影響を受けるシステムを利用している場合、速やかな対応が必要です。

●最新アップデートの適用

The Apache Software Foundation より公開されている本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。

-Apache HTTP Server 2.4.51

●入力内容を確認する

パストラバーサル攻撃でよく用いられる「../」といった文字が含まれていないかチェックし含まれていた場合、直接実行されないシステムの構築が攻撃への対策につながります。

●Web サーバ内のファイル名を外部からのパラメータで直接指定できない設計を行う

パストラバーサルは非公開ファイルの名前を外部からパラメータで指定することでアクセスを試みます。従ってそれを防ぐ設計を行うことで、パストラバーサルの根本的な対策となり得ます。

●ファイルへのアクセス制限の管理を行う

Web サーバ内のファイルへのアクセス制限を正しく設定することで、攻撃者が任意のディレクトリのファイルを指定して開こうとしても、そのアクセスを拒否できる可能性があります。

●セキュリティ機器による攻撃通信の監視

WAF(Web Application 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. 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/

8. 参考情報

・JPCERT/CC

Apache HTTP Server のパストラバーサルの脆弱性（CVE-2021-41773）に関する注意喚起

https://www.jpcert.or.jp/at/2021/at210043.html

・IPA

更新：Apache HTTP Server の脆弱性対策について(CVE-2021-41773, CVE-2021-42013)

https://www.ipa.go.jp/security/ciadr/vul/alert20211006.html

安全なウェブサイトの作り方 - 1.3 パス名パラメータの未チェック／ディレクトリ・トラバーサル

https://www.ipa.go.jp/security/vuln/websecurity-HTML-1_3.html

・Netcraft

October 2021 Web Server Survey

https://news.netcraft.com/archives/2021/10/15/october-2021-web-server-survey.html

※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