SoftBank Technology

ソフトバンク・テクノロジー株式会社

脆弱性調査レポート

Apache HTTP Server の脆弱性により、権限昇格可能な脆弱性(CVE-2019-0211)に関する調査レポート

【概要】

Apache HTTP Serve に、ローカルから権限昇格を行える脆弱性（CVE-2019-0211）及び、その脆弱性を利用する攻撃コードが発見されました。この脆弱性は Apache HTTP Server が再起動を行う際に、子プロセスの境界値チェックが行われていないことにより発生します。これにより、システム上で権限昇格を行うことが可能となります。

攻撃者がこの脆弱性を利用するためには、システムへの有効なログオン情報が必要になります。
Apache HTTP Server の親プロセスが root 権限で動作しているシステムにおいて、攻撃者が何らかの方法でシステムの一般ユーザーでのアクセス権を獲得した場合、この脆弱性を利用することで管理者権限を掌握される可能性があります。その結果、管理者権限でシステムを操作し、重要情報の改ざん、窃取されてしまうといった危険性があります。
また、脆弱性の影響を受ける Apache HTTP Server を利用している共有ホスティングサービスにおいては、ホスティングを利用するユーザーがこの脆弱性を利用することにより、ホスティングサービスを利用する他のユーザーも侵害を受ける可能性があります。

本レポート作成（2019 年 4 月 25 日）時点において、Apache Software Foundation よりこの脆弱性が修正されたバージョンがリリースされております（2019 年 4 月 1 日付）。しかしながら、攻撃が容易であり、かつ攻撃コードも公開されていること、また攻撃を受けた際にシステムへの影響が大きいこと、加えて HTTP Server としてシェアが大きい Apache HTTP Server がターゲットであることから、今回、この脆弱性（CVE-2019-0211）の再現性について検証を行いました。

【影響を受ける可能性があるシステム】

- Apache HTTP Server 2.4.17 から 2.4.38 までのバージョン

【対策案】

本レポート作成（2019 年 4 月 25 日）時点において、Apache Software Foundation より、この脆弱性を修正するバージョンがリリースされています。当該脆弱性が修正されたバージョンへとアップグレードしていただくことを推奨いたします。

【参考サイト】

- CVE-2019-0211
- Apache HTTP Server 2.4 vulnerabilities

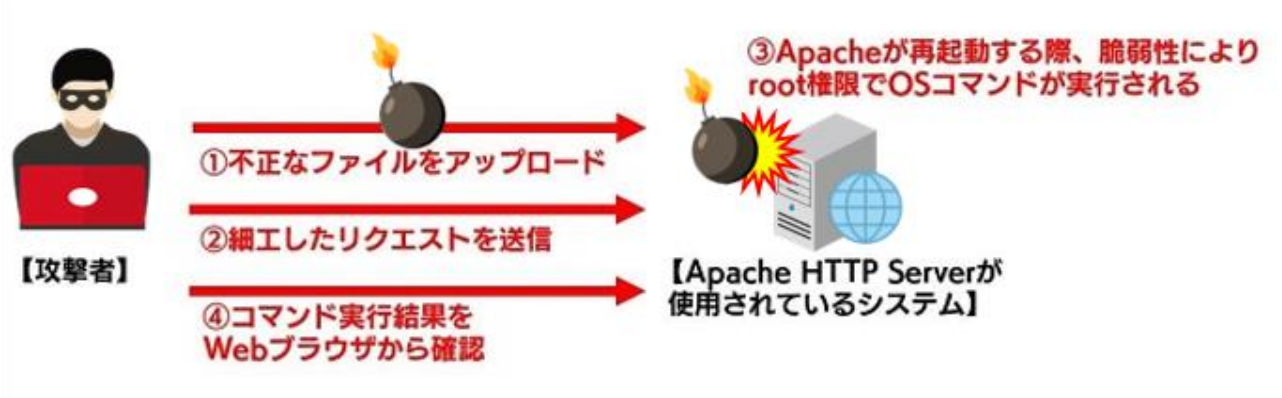
【検証概要】

予め、ターゲットシステム上で動作している脆弱な Apache HTTP Server の公開ディレクトリ上に、不正なコードを実行するためのファイルを配置します。次に、ブラウザ上から先ほど配置したファイルに対し、URL の後ろに任意の OS コマンドを追加してアクセスを行います。今回の検証では、root 権限のみアクセス可能な/etc/shadow ファイルの内容を Apache HTTP Server の公開ディレクトリ上に作成するというコマンドを実行しています。
その後、Apache HTTP Server を再起動し、ブラウザから作成されたファイルの URL にアクセスすることにより、任意の OS コマンドの実行結果を確認します。

【検証ターゲットシステム】

Ubuntu 18.04 上で動作する Apache 2.4.29 および PHP 7.2.15

【検証イメージ】



【検証結果】

以下の画面は、ターゲットシステム上で稼動する Apache HTTP Server の公開ディレクトリ上に作成された /etc/shadow ファイルの内容をブラウザで表示したものです。通常、Apache HTTP Server の動作権限では /etc/shadow ファイルの内容を参照することはできませんが、脆弱性を利用することによりファイルの内容を表示することが可能です。

【更新履歴】

2019 年 4 月 26 日 ： 初版公開

ソフトバンク・テクノロジー株式会社
〒160-0022 東京都新宿区新宿 6 丁目 27 番地 30 号
新宿イーストサイドスクエア 17 階
受付時間：平日 10:00～17:00
電話 03-6892-3154
メール sbt-ipsol@tech.softbank.co.jp
URL https://www.softbanktech.co.jp/