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

Apple Script Editor の脆弱性により、リモートから任意のコードを実行可能な脆弱性（CVE-2015-7007）、および、rsh の脆弱性により、権限昇格が行える脆弱性（CVE-2015-5889）に関する調査レポート

【概要】

Apple OS X に、リモートより任意のコードが実行される脆弱性（CVE-2015-7007）の攻撃コード、および、ローカルから権限昇格を行える脆弱性（CVE-2015-5889）の攻撃コードが発見されました。

CVE-2015-7007 の脆弱性は、URL が applescript://の内容を Script Editor で開く際に、ユーザーの確認なしに内容を実行してしまうために発生します。また、CVE-2015-5889 の脆弱性は、rsh の環境変数の設計に不備があるために発生します。

これらの脆弱性を利用した攻撃が成立した場合、リモートから Script Editor を実行できるアプリケーション（例えば Safari）を実行するユーザーの権限を奪取された後に、権限昇格を行われ、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。

本レポート作成（2015 年 11 月 2 日）時点において、既に Apple よりこれら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（2015 年 10 月 26 日）。しかしながら、攻撃を成立させるためのコードが容易に入手可能であり、かつ攻撃が容易であること、また攻撃を受けた際にシステムへの影響が大きいことから、今回、これらの脆弱性（CVE-2015-7007）（CVE-2015-5889）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】

（CVE-2015-7007 の場合）

- OS X El Capitan 10.11
- ※弊社検証において、OS X Yosemite 10.10.5 でも影響を受けることを確認しております。

（CVE-2015-5889 の場合）

- OS X Snow Leopard 10.6.8 から OS X Yosemite 10.10.5

【対策案】

本レポート作成（2015 年 11 月 2 日）時点において、Apple 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。

なおこれらの脆弱性は、OS X 10.10.x よりも前のバージョンには、脆弱性を修正するパッチがリリースされていません。該当するバージョンを利用されている場合、これらの脆弱性を修正するためには、バージョン 10.11.1 へとアップグレードしていただく必要があります。

【参考サイト】

（CVE-2015-7007）

- CVE-2015-7007
- Apple OS X のスクリプトエディタにおける AppleScript の実行でユーザ確認の要求を回避される脆弱性
- About the security content of OS X El Capitan v10.11.1 and Security Update 2015-007

（CVE-2015-5889）

- CVE-2015-5889
- Apple OS X の remote_cmds コンポーネントの rsh における root 権限を取得される脆弱性
- OS X El Capitan v10.11 のセキュリティコンテンツについて

【検証概要】

ターゲットシステムを攻撃者が用意したサイトにアクセスさせることで、リモートから任意のコードが実行可能な脆弱性（CVE-2015-7007）を利用して任意のコードを実行させます。

今回の検証に用いたコードは、ターゲットシステム上から特定のサーバー、ポートにコネクションを確立させるよう誘導し、システム制御を奪取するものです。これにより、リモートからターゲットシステムが操作可能となります。

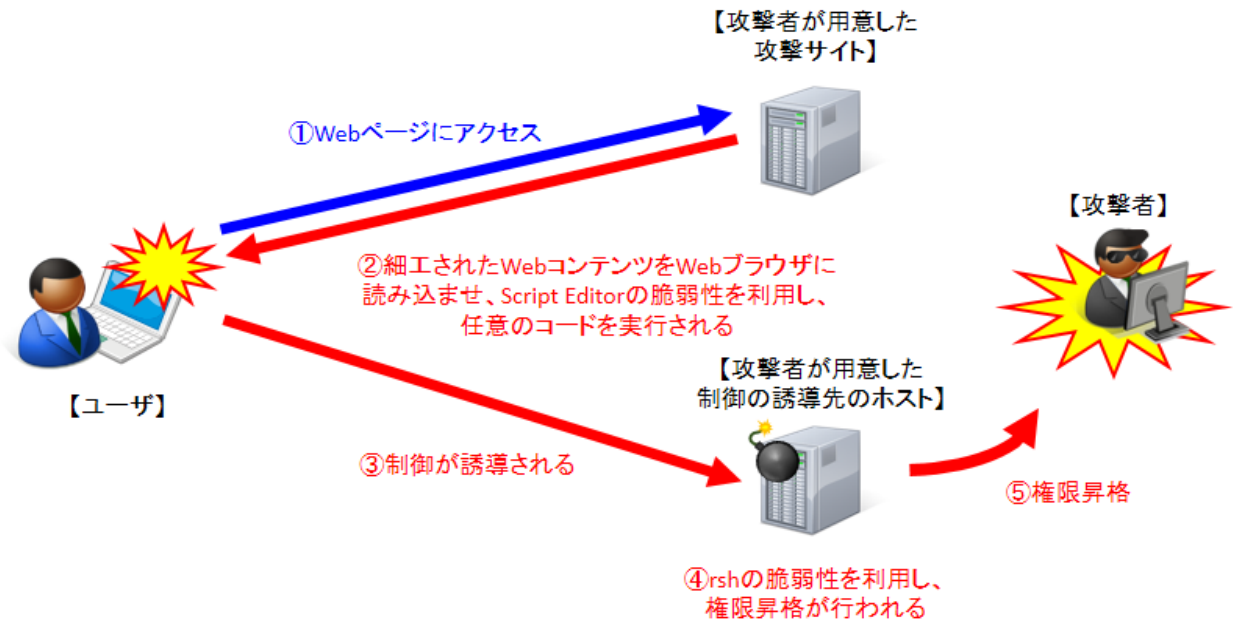
その後、権限昇格が行える脆弱性（CVE-2015-5889）を利用して、root 権限の奪取を試みます。

*誘導先のシステムは Linux です。

【検証ターゲットシステム】

Mac OS X 10.10.5

【検証イメージ】

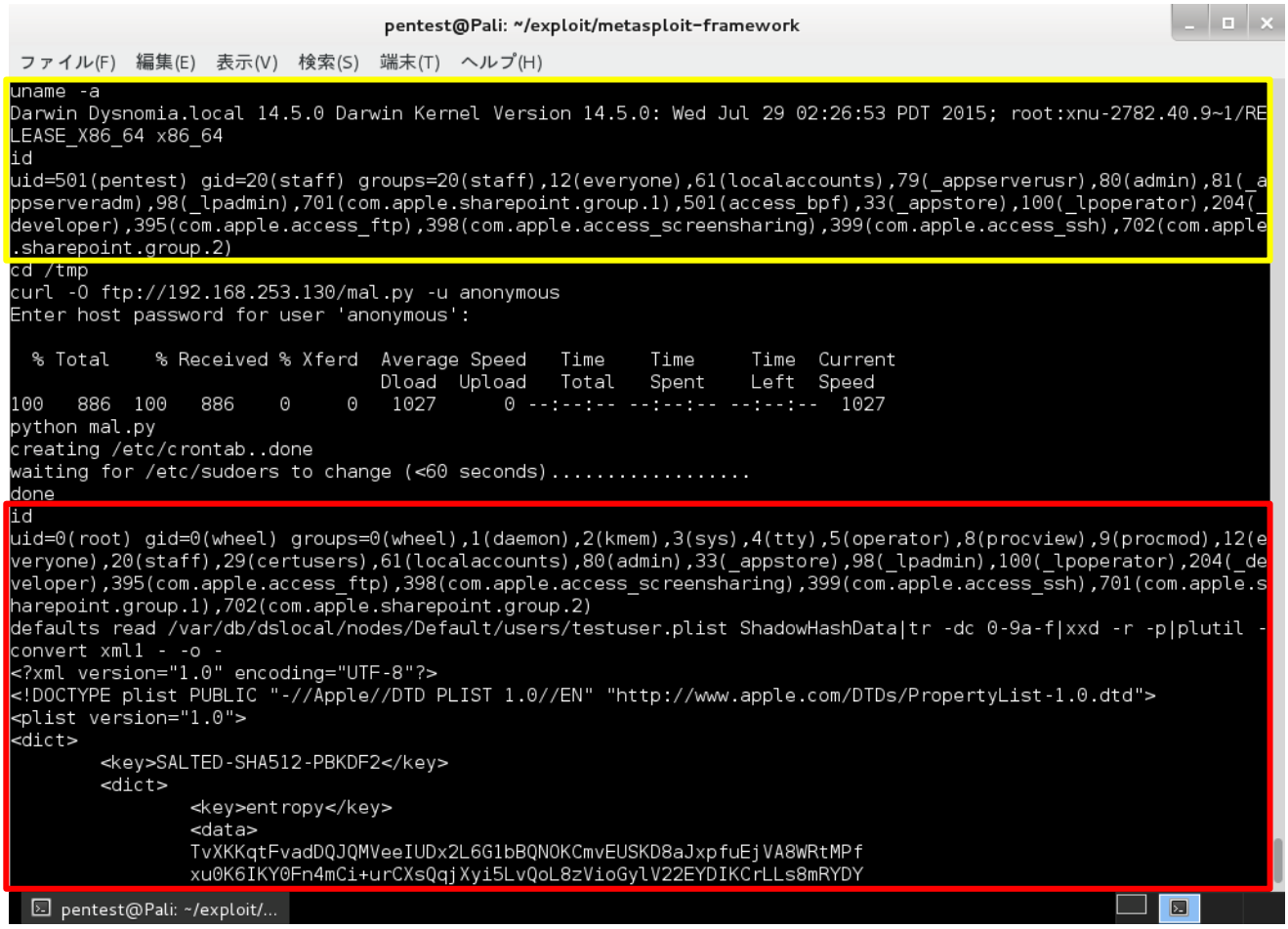


【検証結果】

下図は、誘導先のコンピュータ（Linux）のターミナルの画面で、ターミナル上でターゲットシステムの制御を奪取した状態です。

黄線で囲まれた部分は、リモートから任意のコードが実行可能な脆弱性（CVE-2015-7007）を利用してターゲットシステムの制御を奪取した直後のもので、ホスト情報の他に奪取した一般ユーザー（pentest ユーザー）の情報が表示されています。

一方で、赤線で囲まれている部分は、権限昇格が行える脆弱性（CVE-2015-5889）を利用して、一般ユーザーから管理者権限ユーザーである root へと昇格を行っています。ユーザーの情報を表示するコマンドにより、root 権限へ昇格できていることが確認できます。



【更新履歴】

2015 年 11 月 2 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.jp/