NTTデータ 先端技術株式会社

Firefox の不具合により、chrome 特権機能へのアクセスが制限されず 任意のコードが実行される脆弱性(CVE-2013-0757)(CVE-2013-0758)に関する検証レポート

2013/05/31
NTT データ先端技術株式会社
辻　伸弘
渡邊　尚道

【概要】

Firefox にリモートより任意のコードが実行される脆弱性が発見されました。

本脆弱性は、Chrome Object Wrapper (COW)の実装の不具合によって、chrome 特権へのアクセス制限が回避される問題(CVE2013-0757)及び、SVG オブジェクト経由でのコードの実行が制限されない問題(CVE-2013-0758) が原因で、chrome 特権にて任意のコードが実行されることによりおこります。

この脆弱性により、リモートから Firefox を実行するローカルユーザと同じ権限で任意のコードを実行される危険性があります。
攻撃者は、特別に細工した Web サイトにユーザを誘導させたり、ドキュメント内で Firefox を実行させるような細工したファイルを添付した電子メールを送信し、被攻撃者がファイルを開くことで、ログオンしているユーザと同じ権限を奪取される危険性があります。

今回、Firefox の Chrome Object Wrapper (COW)の実装の不具合によって、chrome 特権へのアクセス制限が回避される問題(CVE2013-0757)と、SVG オブジェクト経由でのコードの実行が制限されない問題(CVE-2013-0758)の再現性について検証を行いました。

【影響を受けるとされているシステム】

影響を受ける可能性が報告されているのは次の通りです。

- Firefox 18.0 未満のバージョン
- Firefox ESR 17.0.2 未満のバージョン
- Thunderbird 17.0.2 未満のバージョン
- Thunderbird ESR 17.0.2 未満のバージョン
- SeaMonkey 2.15 未満のバージョ

【対策案】

Mozilla プロジェクトより、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最新のバージョンにアップデートしていただくことを推奨いたします。

Firefox のダウンロードサイト
http://www.mozilla.jp/firefox/

【参考サイト】

CVE-2013-0757
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-0757

Mozilla Foundation セキュリティアドバイザリ 2013-14
http://www.mozilla-japan.org/security/announce/2013/mfsa2013-14.html

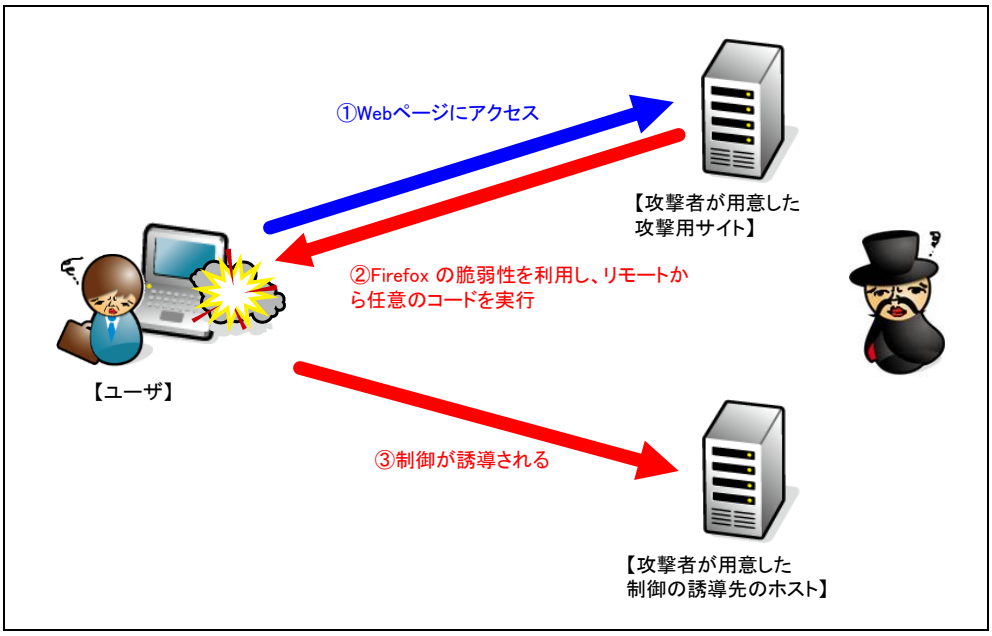
JVNDB-2013-001073 - JVN iPedia - 脆弱性対策情報データベース
http://jvndb.jvn.jp/ja/contents/2013/JVNDB-2013-001073.html

CVE-2013-0758
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-07578

Mozilla Foundation セキュリティアドバイザリ 2013-15
http://www.mozilla-japan.org/security/announce/2013/mfsa2013-15.html

JVNDB-2013-001079 - JVN iPedia - 脆弱性対策情報データベース
http://jvndb.jvn.jp/ja/contents/2013/JVNDB-2013-001079.html

【検証イメージ】



【検証ターゲットシステム】

Windows 7 上の Firefox 17.0.1

【検証概要】

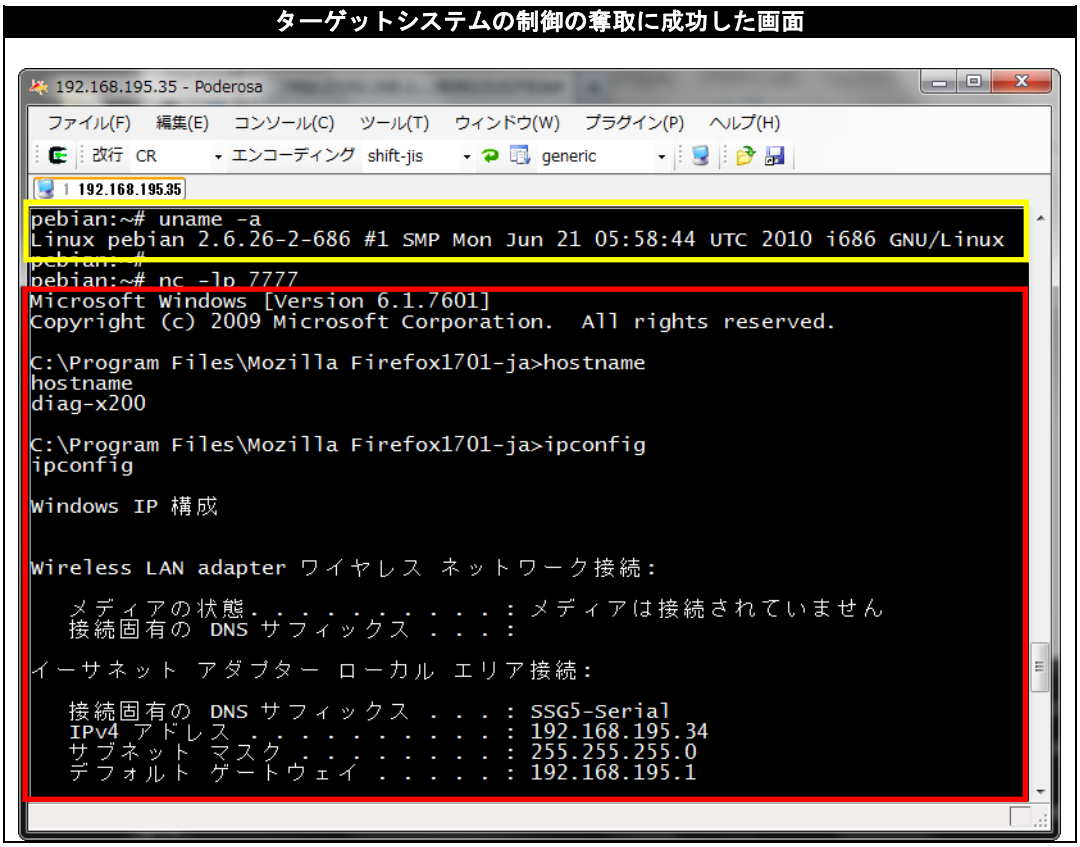
ターゲットシステム上で、攻撃者が作成した Web ページを閲覧させることで、攻撃コードを実行させます。それによって、ターゲットシステムにおいて任意のコードを実行させます。
ターゲットシステムは、攻撃者が用意したホストに制御が誘導されます。
今回の検証に用いたコードは、ターゲットシステム上から特定のサーバ、ポートへコネクションを確立させるよう誘導し、システムの制御を奪取するものです。
これにより、リモートからターゲットシステムが操作可能となります。
＊誘導先のシステムは Debian です。

【検証結果】

下図は、攻撃後の誘導先のコンピュータ（Debian）の画面です。黄線で囲まれている部分は、誘導先のコンピュータのホスト情報です。一方、赤線で囲まれている部分は、ターゲットシステム（Windows 7）において、コマンドを実行した結果が表示されています。

これにより、ターゲットシステムの制御の奪取に成功したと言えます。

ターゲットシステムの制御の奪取に成功した画面



＊各規格名、会社名、団体名は、各社の商標または登録商標です。

【お問合せ先】

NTT データ先端技術株式会社
セキュリティ事業部
TEL:03-5859-5422
http://security.intellilink.co.jp