NTTデータ・セキュリティ株式会社

Firefox の location オブジェクト処理の脆弱性(CVE-2009-3985)に関する検証レポート

2009/12/22
診断ビジネス部
辻　伸弘
松田　和之

【概要】

Firefox の location オブジェクト処理に脆弱性が存在することが発見されました。
この脆弱性により、Web ページの閲覧、HTML 形式の電子メールの表示、または、電子メールの添付ファイルなどの経路から細工された HTML ファイルを閲覧した場合に、ブラウザのアドレスバーに表示される URL を詐称される恐れがあります。
想定される被害としては、フィッシングにより、ユーザ情報、クレジットカード情報等を窃取されることが考えられます。

今回、Firefox の location オブジェクト処理の脆弱性（CVE-2009-3985）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】

Firefox 3.0.16 より前のバージョン
Firefox 3.5.6 より前のバージョン

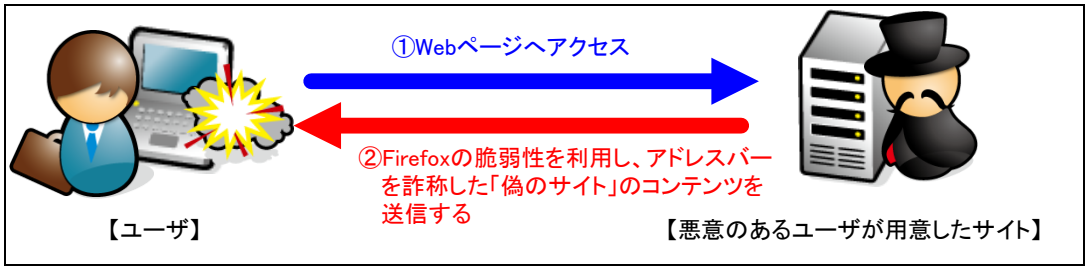
【対策案】

修正されたバージョンFirefox 3.0.16、及び、3.5.6 以上がリリースされております。
修正されたバージョンにアップデートすることが推奨されます。

【参考サイト】

CVE-2009-3985
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-3985

【検証イメージ】



【検証ターゲットシステム】

Firefox 3.0.15 がインストールされた Windows XP

【検証概要】

ターゲットシステム上で、細工した HTML ファイルを表示することでアドレスバーに表示される URL を詐称します。
本検証に用いたコードは、ターゲットシステム上のアドレスバーに表示される URL を「https://www.google.com /」に詐称するものです。

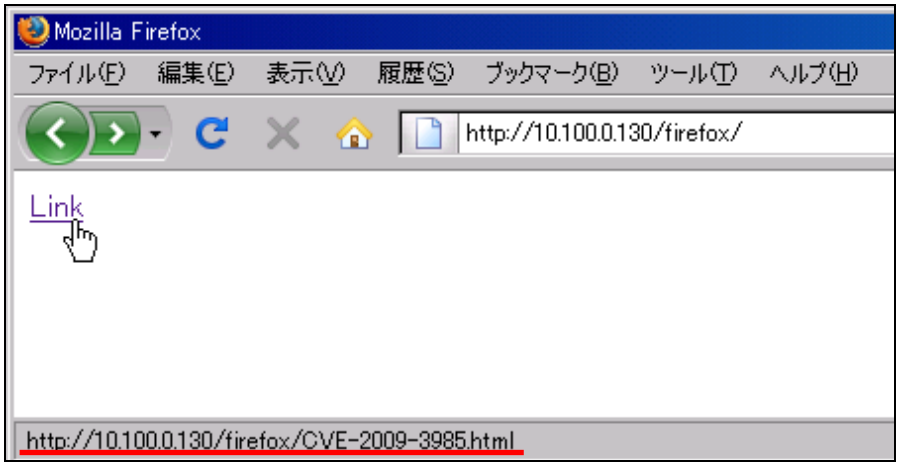
Copyright © 2009. NTT DATA SECURITY CORPORATION All right reserved.

NTTデータ・セキュリティ株式会社

【検証結果】

下図の赤線が示すように、リンク先のアドレスは「http://10.100.0.130/firefox/CVE-2009-3985.html」を示しています。
リンク先の細工された HTML ファイルにより、Firefox の location オブジェクト処理の脆弱性を利用し、アドレスバーに表示される URL の詐称を試みます。

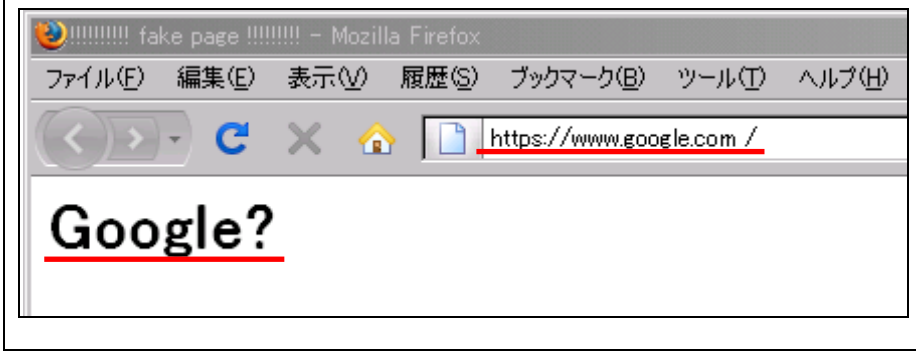
細工した HTML ファイルにアクセスする画面



下図は、細工した HTML ファイルにアクセスした後の画面です。赤線が示すように、ターゲットシステムのブラウザのアドレスバーに表示される URL が「https://www.google.com/」に詐称され、攻撃者が用意した「偽サイト」のコンテンツが表示されています。
これにより、ターゲットシステムのアドレスバーに表示される URL の詐称に成功したと言えます。
URL を詐称されることにより、フィッシングに利用され、ユーザ情報、クレジットカード情報等を窃取される危険性があります。

※なお、詐称に成功した URL の末尾にはスペース文字が含まれております。

アドレスバーに表示される URL を詐称した画面



＊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・セキュリティ株式会社
営業企画部
TEL:03-5425-1954
http://www.nttdata-sec.co.jp/

Copyright © 2009. NTT DATA SECURITY CORPORATION All right reserved.