NTTデータ先端技術株式会社

Firefox の nsTreeRange オブジェクトにおけるメモリ破壊の脆弱性（CVE-2011-0073）に関する検証レポート

2011/07/14
NTT データ先端技術株式会社
辻　伸弘
小田切　秀暁

【概要】

Firefox にリモートから攻撃可能なメモリ破壊の脆弱性（CVE-2011-0073）が発見されました。
この脆弱性は Firefox の nsTreeRange オブジェクトの処理に起因します。Firefox が削除されたオブジェクトを誤って処理してしまうため、メモリ破壊を引き起こす可能性があります。
この脆弱性により、細工された Web ページの閲覧などで、ローカルユーザと同じ権限が奪取される危険性があります。想定される被害としては、ローカルユーザ権限での情報取得、改ざん、または、ワームやスパイウェアなどの悪意あるプログラムをシステム内にインストールされることが考えられます。

今回、この Firefox の脆弱性（CVE-2011-0073）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アプリケーション】

現在のところ、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 3.5.19 以前のバージョン
・Firefox 3.6.17 以前のバージョン
・SeaMonkey 2.0.14 以前のバージョン

【対策案】

修正されたバージョン Firefox 3.5.19、3.6.17 および SeaMonkey 2.0.14 以上がリリースされています。修正されたバージョンにアップデートすることを推奨いたします。

【参考サイト】

Bugzilla@Mozilla – Bug 630919
https://bugzilla.mozilla.org/show_bug.cgi?id=630919

CVE-2011-0073
http://cve.mitre.org/cgi-bin/cvename.cgi?name=2011-0073

【検証イメージ】

【検証ターゲットシステム】

Windows XP Professional SP3 および Firefox 3.6.12

NTTデータ先端技術株式会社

【検証概要】

ターゲットシステムに Firefox を通じて、細工された Web ページを閲覧させ、Firefox の脆弱性を利用した攻撃コードを実行することで任意のコードを実行させます。

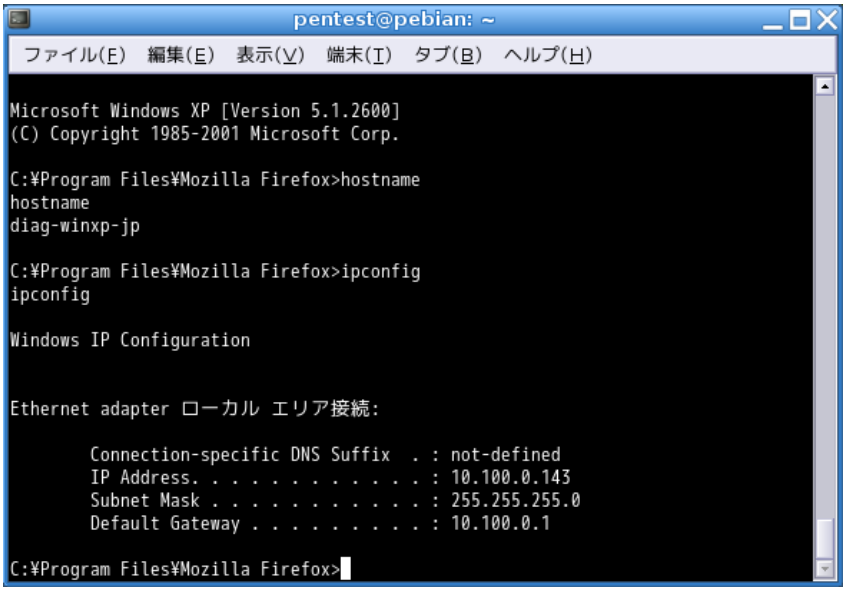
今回の検証に用いたコードは、ターゲットシステム上から特定のサーバ、ポートへコネクションを確立させるように誘導し、システムの制御を奪取するものです。
これにより、リモートからターゲットシステムの操作が可能となります。
＊ 誘導先のシステムは Linux です。

【検証結果】

下図が示すように、誘導先のコンピュータ（Debian）上にターゲットシステム（Windows XP）のプロンプト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　営業担当　営業企画グループ
TEL：03-5425-1954
http://security.intellilink.co.jp/