NTTデータ・セキュリティ株式会社

複数の脆弱性(MS06-014, MS07-004, MS07-017)を利用した攻撃コード生成ツールに関する検証レポート

2007/04/17
NTT データ・セキュリティ株式会社
辻 伸弘

【概要】

Windows の脆弱性を利用した攻撃コードを容易に生成可能なツールが発見されました。
ツールの仕様としては、Web ページを閲覧したユーザのコンピュータ上で実行させたい任意のプログラムの URL を指定し、ボタンをクリックするだけで攻撃コードが生成されます。専門的な知識を必要とせず、簡単に悪意のあるページを生成することが可能です。
悪意のあるユーザは、この任意のプログラムにワームやボット、スパイウェアなど悪意のあるプログラムを指定します。
そして、メールや掲示板を利用したハイパーリンクなどの方法でユーザを巧妙にページの閲覧へと誘導します。
脆弱性が修正されていないコンピュータで悪意のあるページを閲覧したユーザは、システムの乗っ取り、情報の搾取などを行われることとなります。

ツールによって利用されている脆弱性は 3 種類です。各脆弱性の情報は以下サイトをご覧ください。

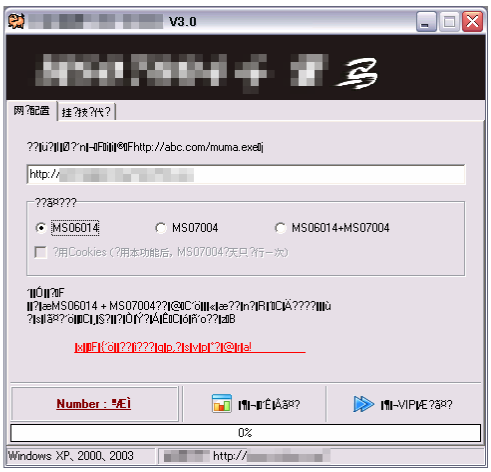
・Microsoft Data Access Components (MDAC) の機能の脆弱性により、コードが実行される可能性がある(911562) (MS06-014)
http://www.microsoft.com/japan/technet/security/bulletin/ms06-014.mspx

・Vector Markup Language の脆弱性により、リモートでコードが実行される (929969) (MS07-004)
http://www.microsoft.com/japan/technet/security/bulletin/ms07-004.mspx

・GDI の脆弱性により、リモートでコードが実行される (925902) (MS07-017)
http://www.microsoft.com/japan/technet/security/bulletin/ms07-017.mspx

今回、このツールによる脆弱性を利用した攻撃の再現性について検証を行いました。

検証に使用した悪意のあるページを作成するツール



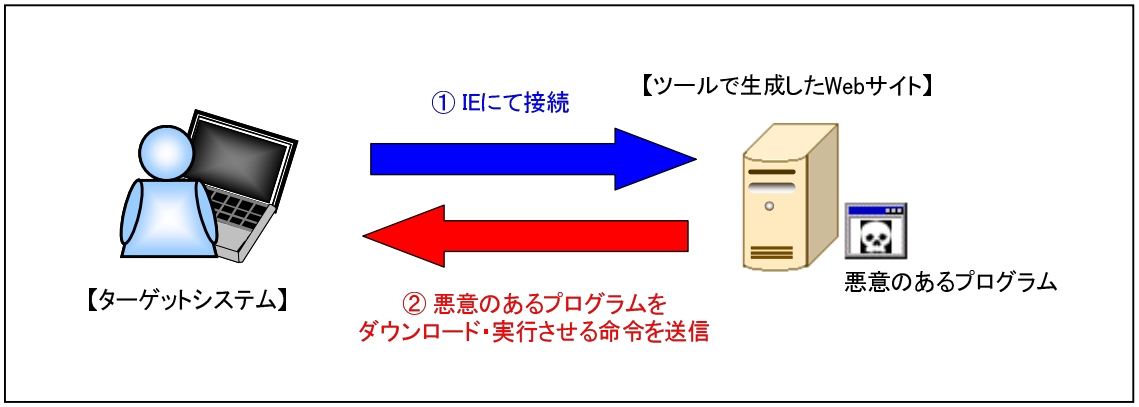
NTTデータ・セキュリティ株式会社

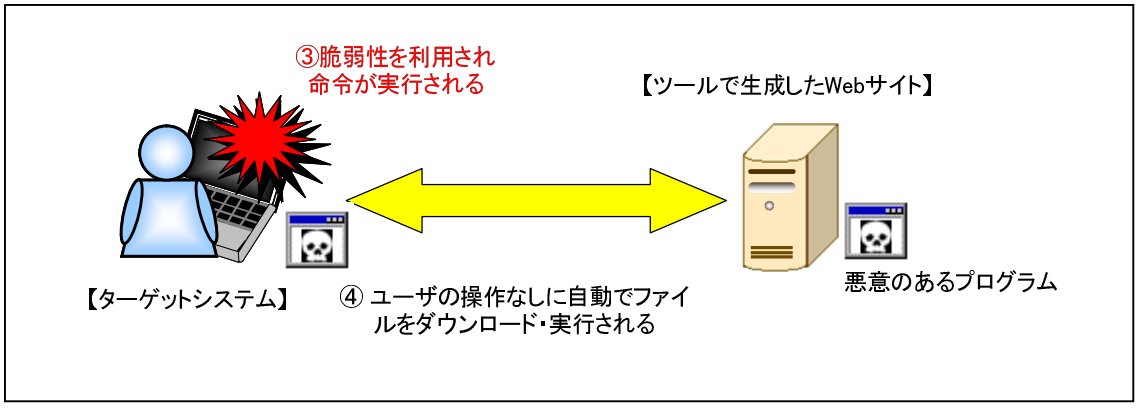
【検証ターゲットシステム】
Windows XP Professional（日本語版） + Service Pack2
（該当脆弱性の各修正プログラム未適用の 3 パターンで検証）

【検証アタックシステム】
Fedora Core 4 上に構築した Apache 上に検証用ページを用意

【検証概要】
ターゲットシステム上の Internet Explorer にて、ツールにより生成したページを閲覧し、予めアタックシステム上に用意した実行形式ファイル（EXE ファイル）がターゲットシステム上で実行されるか否かの確認を行いました。

【検証イメージ】



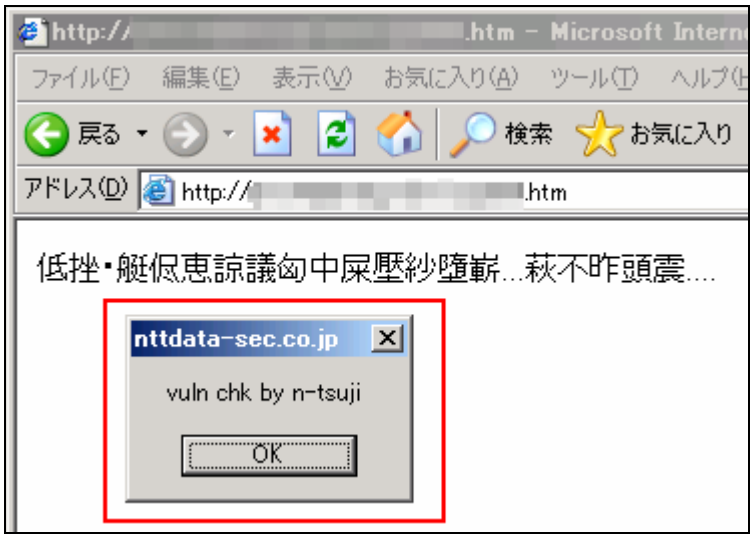


【検証結果】

下図のように、ツールにより作成したページの閲覧後、ユーザによる操作なしに予め用意したプログラムをターゲットシステム上で実行することに成功しました。

赤線で囲われた部分が今回の検証で使用し、実行に成功したプログラムです。

プログラムの実行に成功



今回の検証では、3 種類の修正プログラム未適用状態のパターンを検証しました。
それぞれのパターンについての結果は以下の通りです。

未適用の修正プログラム	結果
MS06-014	**プログラムの実行に成功**
MS07-004	**Internet Explorer が異常終了**
MS07-017	プログラムは実行に失敗

【対策案】

充分な検証の後、運用に支障をきたさないことをご確認の上、各修正プログラムの適用を行ってください。

【見解】

専門的な知識を必要とせず、非常に簡単な操作のみで悪意のあるページを作成できることが、今回の検証で明らかになりました。このようなツールはコンピュータアンダーグラウンドサイトにて、無料で誰もが手に入れることが可能な状態となっております。
そのため、弊社で確認した限りでも、このソフトを利用したと思われる悪意のあるページが世界中に多数存在し、増え続ける傾向にあります。
悪意のあるページによる被害に遭わないためには、今一度、管理下のネットワーク上のコンピュータに対し、修正プログラムの適用状況をご確認いただき、適用されていない場合は早急に対処いただくことが推奨されます。

NTTデータ・セキュリティ株式会社

【参考ページ】
マイクロソフト セキュリティ情報

・Microsoft Data Access Components (MDAC) の機能の脆弱性により、コードが実行される可能性がある (911562) (MS06-014)
http://www.microsoft.com/japan/technet/security/bulletin/ms06-014.mspx

・Vector Markup Language の脆弱性により、リモートでコードが実行される (929969) (MS07-004)
http://www.microsoft.com/japan/technet/security/bulletin/ms07-004.mspx

・GDI の脆弱性により、リモートでコードが実行される (925902) (MS07-017)
http://www.microsoft.com/japan/technet/security/bulletin/ms07-017.mspx

＊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/