NTTデータ・セキュリティ株式会社

IE6 のクロスドメインスクリプティングの脆弱性に関する検証レポート

2008/7/7
診断ビジネス部
辻　伸弘
松田　和之

【概要】

Internet Explorer6(以下 IE6)のウィンドウオブジェクト「location」、及び、「location.href」プロパティの入力検証処理にクロスドメインスクリプティングの脆弱性が発見されました。
クロスドメインスクリプティングとは、異なるドメイン間で任意のスクリプトを実行可能である脆弱性を指します。想定される被害としては、悪意のあるユーザにより、信頼できるサイトで利用している Cookie 情報が窃取されることが挙げられます。(「被害イメージ」参照)

この脆弱性は、IE6 のドメイン間のセキュリティモデルが正しく機能していないことに起因しております。
よって、クロスサイトスクリプティングとは異なり、信頼できるサイト内に脆弱性が存在しない場合でも、クロスドメインスクリプティング攻撃の影響を受けるため、注意が必要です。

今回、IE6 のクロスドメインスクリプティングの脆弱性についての調査を行いました。

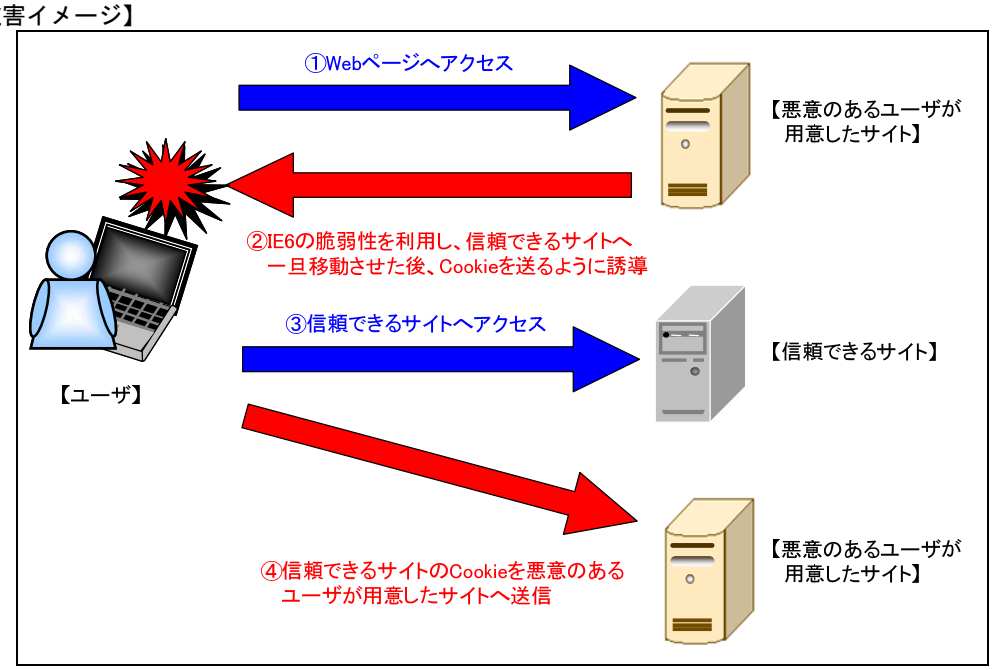
【影響を受けるとされているシステム】

Microsoft Internet Explorer 6

【対策案】

このレポート作成現在（2008 年 7 月 7 日)、ベンダーより、IE6 に対する修正プログラムはリリースされておりません。修正プログラムのリリース、適用までは、怪しいサイトやメールの閲覧を行わない、アクティブスクリプトを無効にする、または、Internet Explorer 7 へアップデートすることを推奨いたします。

【被害イメージ】



【検証ターゲットシステム】
Microsoft Internet Explorer 6 がインストールされた Windows XP Service Pack 2
(Version: 6.0.2900.2180.xpsp_sp2_qfe.070227-2300)

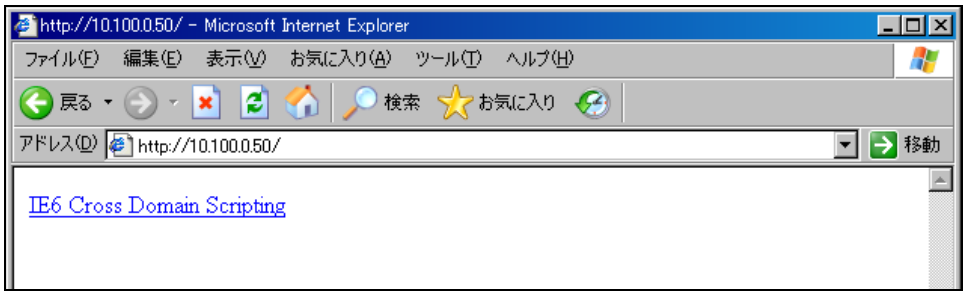
【検証概要】
ターゲットシステムに、悪意のあるユーザが用意したサイトにアクセスさせることで、信頼できるサイトの Cookie を取得します。今回の検証に用いたスクリプトは、異なるドメインで利用している Cookie を悪意のあるユーザが用意したサイトへ送信するものです。(「被害イメージ」参照)

【検証結果】
以下に、被害イメージの流れに沿って検証を行いました。

検証結果中のブラウザに表示されているアドレスは下記の意味を持っています。

10.100.0.50 : 悪意のあるユーザが用意したサイト
10.100.0.100 : 信頼できるサイト

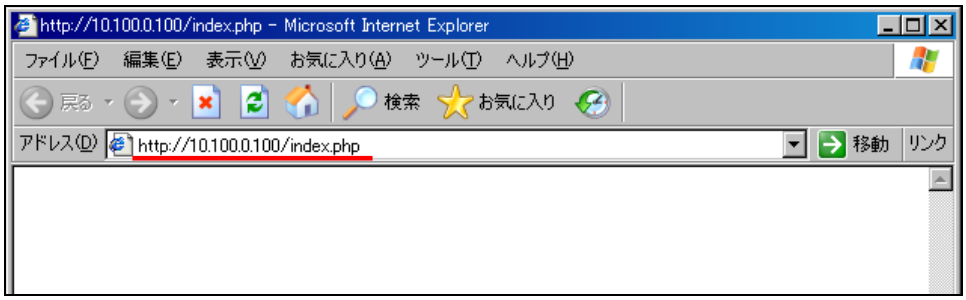
①Web ページへアクセス



上図は、IE6 を使用し、悪意のあるユーザが用意したサイト「10.100.0.50」へアクセスした画面を示しています。
(被害イメージ①)

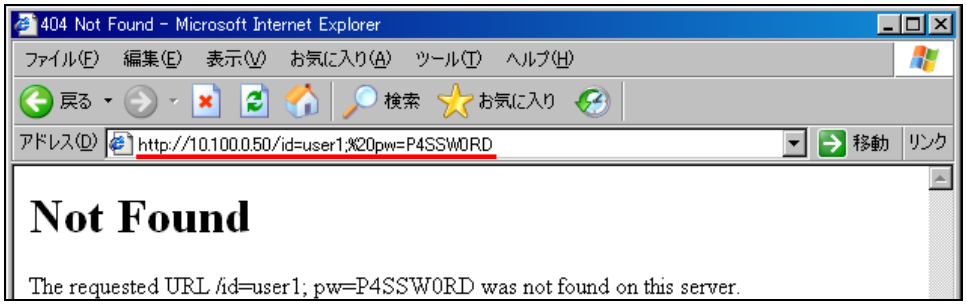
ユーザが、「IE6 Cross Domain Scripting」と書かれたリンクをクリックすると、IE6 の脆弱性を利用したスクリプトにより、信頼できるサイトへ一旦移動させた後、悪意のあるユーザが用意したサイトへ Cookie を送信するよう誘導させられます。
(被害イメージ②)

③信頼できるサイトへアクセス



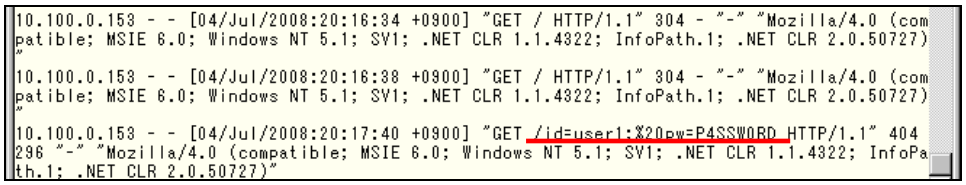
上図は、スクリプトにより、信頼できるサイト「10.100.0.100」へアクセスさせられた際の画面を示しています。
(被害イメージ③)
この段階で、信頼できるサイトで使用されている Cookie 情報が読み出されます。
悪意のあるユーザが用意したサイトへ Cookie 情報を送信する準備段階であると言えます。

④信頼できるサイトの Cookie を悪意のあるユーザが用意したサイトへ送る



上図は、スクリプトにより、自動的に悪意のあるユーザが用意したサイトへ、信頼できるサイトで利用している Cookie 情報を URL に付加してアクセスさせられた際の画面を示しています。
（被害イメージ④）

悪意のあるユーザが用意したサイトのアクセスログ



上図の赤線で示したとおり、悪意のあるユーザが用意したサイトのアクセスログに、信頼できるサイトの Cookie 情報が記録されていることを示しています。このように、悪意のあるユーザは、取得した Cookie を利用し、なりすましを行うことが可能であると判断できます。

【対策案】

このレポート作成現在（2008 年 7 月 7 日）、ベンダーより、IE6 に対する修正プログラムはリリースされておりません。修正プログラムのリリース、適用までは、怪しいサイトやメールの閲覧を行わない、アクティブスクリプトを無効にする、または、Internet Explorer 7 へアップデートすることが推奨されます。

【参考サイト】

Japan Vulnerability Notes
http://jvn.jp/cert/JVNVU923508/index.html

US-CERT
http://www.kb.cert.org/vuls/id/923508

＊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/