NTTデータ・セキュリティ株式会社

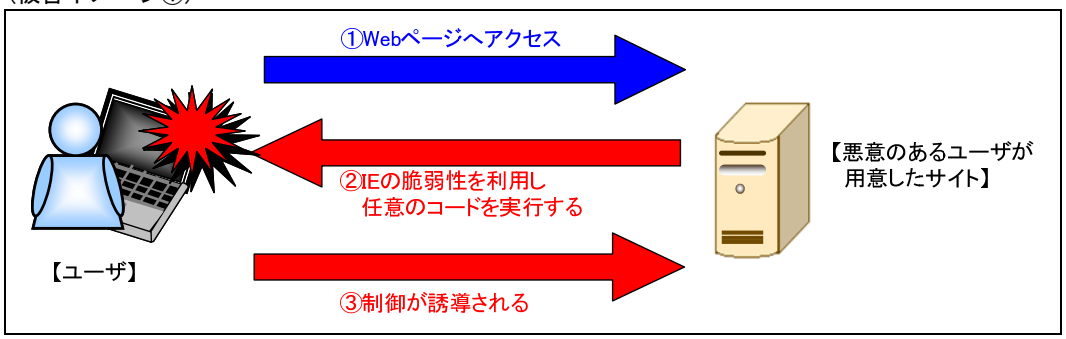
IE のデータバインディング処理の脆弱性に関する検証レポート

2008/12/16
2008/12/18 更新
診断ビジネス部
辻　伸弘
松田　和之

【概要】

Internet Explorer(以下 IE)のデータバインディング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、細工された XML データを含む Web ページの閲覧、HTML 電子メールの表示、または、電子メールの添付を開いた場合に、そのローカルユーザと同じ権限が奪取される恐れがあります。
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。(「被害イメージ①」参照))

(被害イメージ①)

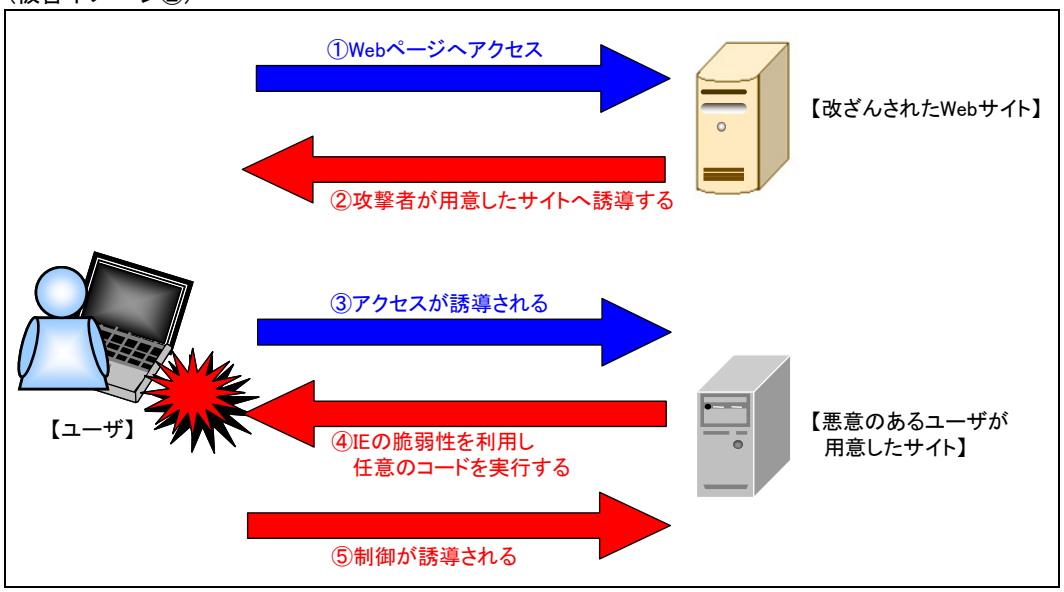


また、SQL インジェクションによって改ざんされたサイトの誘導先にて、今回の脆弱性を利用した攻撃が行われていることも確認されています。ユーザのコンピュータにこの脆弱性が存在する場合、Web サイトにアクセスするだけで、システムの乗っ取りや悪意のあるプログラムのインストールなどが行われる可能性があります。
(「被害イメージ②」参照)

SQL インジェクションによる改ざんについては、以下をご参照ください。

SQL インジェクション・ワームに関する現状と推奨する対策案
http://www.nttdata-sec.co.jp/article/vulner/pdf/report20080529.pdf

(被害イメージ②)



NTTデータ・セキュリティ株式会社

今回、IE のデータバインディング処理の脆弱性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】

以下のエディション上の Internet Explorer 6

- Windows XP SP2/SP3
- Windows XP Professional x64 Edition SP なし/SP2
- Windows Server 2003 SP1/SP2
- Windows Server 2003 with SP1/SP2 for Itanium-based Systems
- Windows Server 2003 x64 Edition SP なし/SP2

以下のエディション上の Internet Explorer 7

- Windows XP SP2/SP3
- Windows XP Professional x64 Edition SP なし/SP2
- Windows Server 2003 SP1/SP2
- Windows Server 2003 with SP1/SP2 for Itanium-based Systems
- Windows Server 2003 x64 Edition SP なし/SP2
- Windows Vista SP なし/SP1
- Windows Vista x64 Edition SP なし/SP1
- Windows Server 2008 for 32-bit Systems
- Windows Server 2008 for Itanium-based Systems
- Windows Server 2008 for x64-based Systems

以下のエディション上の Internet Explorer 8 Beta 2

- Windows XP SP2/SP3
- Windows XP Professional x64 Edition SP なし/SP2
- Windows Server 2003 SP2
- Windows Server 2003 x64 Edition SP なし/SP2
- Windows Vista SP なし/SP1
- Windows Vista x64 Edition SP なし/SP1
- Windows Server 2008 for 32-bit Systems
- Windows Server 2008 for x64-based Systems

【対策案】

このレポート作成現在（2008 年 12 月 15 日）、ベンダーより、IE 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、脆弱性の影響を受けない代替ブラウザを使用する、または、怪しいサイトやメールの閲覧を行わないことが推奨されます。

2008 年 12 月 18 日追記：

Microsoft 社から、修正プログラム（MS08-078）がリリースされています。
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、修正プログラム（MS08-078）の適用を行うことが推奨されます。

http://www.microsoft.com/japan/technet/security/bulletin/ms08-078.mspx

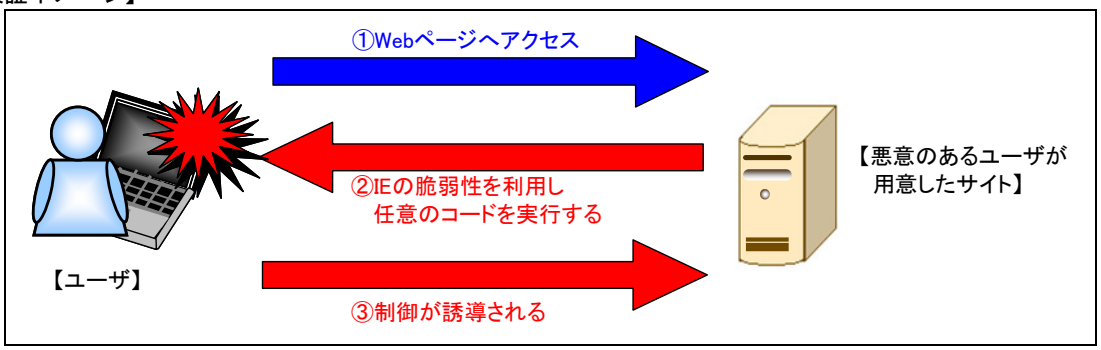
また、マイクロスソフトセキュリティアドバイザリでは、以下の回避策が提示されています。

① インターネット、及び、ローカル イントラネットゾーンの設定を「高」に設定し、これらのゾーンで ActiveX コントロールおよびアクティブスクリプトを実行する前にダイアログを表示する
② インターネット、及び、イントラネットゾーンで、アクティブスクリプトの実行前にダイアログを表示するように Internet Explorer を構成する、または、アクティブスクリプトを無効にするよう構成する
③ Internet Explorer 7 の DEP を有効にする
④ XML アイランド機能を無効にする
⑤ ACL を使用して OLEDB32.DLL を無効にする
⑥ OLEDB32.dll の Row Position 機能を無効にする
⑦ OLEDB32.DLL の登録を解除する
⑧ Internet Explorer 8 Beta 2 のデータバインディングサポートを無効にする

NTTデータ・セキュリティ株式会社

【参考サイト】
マイクロソフト セキュリティ アドバイザリ (961051)
http://www.microsoft.com/japan/technet/security/advisory/961051.mspx

【検証イメージ】



【検証ターゲットシステム】
Microsoft Internet Explorer 7 がインストールされた Windows XP Service Pack 3
(Version: 7.0.5730.13)

【検証概要】
ターゲットシステムに、細工した XML データを含むコンテンツをロードさせ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を操作可能となります。
＊ 誘導先のシステムは CentOS 5 です。

【検証結果】
下図の赤線で囲まれている部分の示すように、誘導先のコンピュータ（CentOS）のコマンドプロンプト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。
黄線で囲まれている部分の示すように、ターゲットシステムにおいて、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

```
[root@localhost ~]# nc -lp 31373
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\Documents and Settings\Administrator\fXNqbv>ipconfig
ipconfig

Windows IP Configuration


Ethernet adapter [J GA:

        Connection-specific DNS Suffix  . : not-defined
        IP Address. . . . . . . . . . . . : 10.100.0.162
        Subnet Mask . . . . . . . . . . . : 255.255.255.0
        Default Gateway . . . . . . . . . : 10.100.0.1

C:\Documents and Settings\Administrator\fXNqbv>
```

NTTデータ・セキュリティ株式会社

【対策案】

このレポート作成現在（2008 年 12 月 15 日）、ベンダーより、IE 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、脆弱性の影響を受けない代替ブラウザを使用する、または、怪しいサイトやメールの閲覧を行わないことが推奨されます。

2008 年 12 月 18 日追記：

Microsoft 社から、修正プログラム（MS08-078）がリリースされています。
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、修正プログラム（MS08-078）の適用を行うことが推奨されます。

http://www.microsoft.com/japan/technet/security/bulletin/ms08-078.mspx

また、マイクロスソフトセキュリティアドバイザリでは、以下の回避策が提示されています。

① インターネット、及び、ローカル イントラネットゾーンの設定を「高」に設定し、これらのゾーンで ActiveX コントロールおよびアクティブスクリプトを実行する前にダイアログを表示する
② インターネット、及び、イントラネットゾーンで、アクティブスクリプトの実行前にダイアログを表示するように Internet Explorer を構成する、または、アクティブスクリプトを無効にするよう構成する
③ Internet Explorer 7 の DEP を有効にする
④ XML アイランド機能を無効にする
⑤ ACL を使用して OLEDB32.DLL を無効にする
⑥ OLEDB32.dll の Row Position 機能を無効にする
⑦ OLEDB32.DLL の登録を解除する
⑧ Internet Explorer 8 Beta 2 のデータバインディングサポートを無効にする

【参考サイト】

マイクロソフト セキュリティ アドバイザリ (961051)
http://www.microsoft.com/japan/technet/security/advisory/961051.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/