Internet Explorer の脆弱性対策について

Internet Explorer に悪意ある細工がされたコンテンツを開くことで任意のコードが実行される脆弱性があることがニュースなどで発表されました。
悪用された場合、攻撃者によってパソコンを制御される可能性があります。

対応策

① セキュリティパッチが配布される予定の 5/14 以降まで以下のような他のブラウザを利用する。
Google Chrome（グーグルクローム） http://www.google.co.jp/intl/ja/chrome/browser/
FireFox（ファイアーフォックス） http://www.mozilla.jp/firefox/

② 現在提供されているセキュリティ対策を適用する（IE に対する対策）
参考 URL
「マイクロソフト Security Tech Center」
（ここに掲載されている推奨するアクション「回避策」のいずれかを実行することによりリスクが緩和します）
https://technet.microsoft.com/library/security/2963983

上記対策の例として以下のものがあります（3 例紹介）

1. VGX.DLL の登録を解除する

[スタート] メニューをクリックし、[ファイル名を指定して実行] をクリックして、"%SystemRoot%¥System32¥regsvr32.exe" -u "%CommonProgramFiles%¥Microsoft Shared¥VGX¥vgx.dll" と入力し、次に [OK] をクリックします。
ダイアログ ボックスに、登録を解除するプロセスが正常に完了したことを確認するメッセージが表示されます。[OK] をクリックして、ダイアログ ボックスを閉じます。

回避策の影響

Vgx.dll の登録が解除されると、VML をレンダリングするアプリケーションはそのレンダリングを行わなくなります、以下は対策の解除方法です。
この問題に対処するセキュリティ更新プログラムが利用可能になったら、そのセキュリティ更新プログラムをインストールした後に vgx.dll を再登録する必要があります。
vgx.dll を再登録するには、次のステップを実行します。

復帰方法（対策解除）

[スタート] メニューをクリックし、[ファイル名を指定して実行] をクリックして、"%SystemRoot%¥System32¥regsvr32.exe" "%CommonProgramFiles%¥Microsoft Shared¥VGX¥vgx.dll" と入力し、次に [OK] をクリックします。
ダイアログ ボックスに、登録するプロセスが正常に完了したことを確認するメッセージが表示されます。[OK] をクリックして、ダイアログ ボックスを閉じます。

2. Enhanced Mitigation Experience Toolkit 4.1 を使用する

Enhanced Mitigation Experience Toolkit (EMET) は、脆弱性の悪用を困難にする保護レイヤーを追加することによって、この脆弱性の悪用を防止するために役立ちます。マイクロソフトは、EMET 4.1 を正式にサポートしています。現時点で、EMET は英語版のみで提供されています。詳細については、サポート技術情報 2458544 を参照してください。

注: EMET 3.0 はこの問題を緩和しません。

適用方法

マイクロソフトの以下のページから Enhanced Mitigation Experience Toolkit 4.1 をダウンロードしてインストールしてください（英語）

http://www.microsoft.com/en-us/download/details.aspx?id=41963

3. インターネットおよびローカル イントラネット セキュリティ 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 スクリプトをブロックする。

インターネット セキュリティ ゾーンの設定を変更し、ActiveX コントロールおよびアクティブ スクリプトをブロックすることは、この脆弱性の悪用を防ぐのに役立ちます。これには、ブラウザのセキュリティ設定を「高」に設定して実行します。

Internet Explorer のブラウザのセキュリティ レベルを上げるには、以下のステップを実行してください。

① Internet Explorer の [ツール] メニューの [インターネット オプション] をクリックします。

② [インターネット オプション] ダイアログ ボックスで、[セキュリティ] タブをクリックし、次に [インターネット] をクリックします。

③ [このゾーンのセキュリティのレベル] の下のスライダーのつまみを「高」まで移動させます。これにより、訪問するすべての Web サイトのセキュリティ レベルが「高」に設定されます。

④ [ローカル イントラネット] をクリックします。

⑤ [このゾーンのセキュリティのレベル] の下のスライダーのつまみを「高」まで移動させます。これにより、訪問するすべての Web サイトのセキュリティ レベルが「高」に設定されます。

⑥ [OK] をクリックし、変更を許可し、Internet Explorer に戻ります。

注: スライダーが表示されていない場合、[既定のレベル] ボタンをクリックし、次にスライダーを「高」に移動させます。

注: セキュリティ レベルを「高」に設定すると、Web ページが正しく動作しない場合があります。この設定の変更後、Web サイトの使用が困難になり、そのサイトが安全だと確信できる場合は、そのサイトを [信頼済みサイト] に追加できます。これにより、セキュリティが「高」に設定されていても、そのサイトが適切に実行されます。

回避策の影響:

ActiveX コントロールおよびアクティブ スクリプトをブロックすると、別の影響があります。インターネットまたはイントラネット上の多くの Web サイトは ActiveX またはアクティブ スクリプトを使用して、追加の機能を提供します。たとえば、**オンラインの電子商取引またはオンライン バンキング サイト**には ActiveX コントロールを使用して、メニュー、注文書、計算書などを提供しているものもあります。ActiveX コントロールまたはアクティブ スクリプトのブロックはグローバル設定であり、すべてのインターネットおよびイントラネット サイトに影響を及ぼします。ActiveX コントロールおよびアクティブ スクリプトをこれらの

Web サイトでブロックしたくない場合、「信頼する Web サイトを Internet Explorer の信頼済みサイト ゾーンに追加する」で説明されているステップを行ってください

信頼する Web サイトを Internet Explorer の信頼済みサイト ゾーンに追加する

インターネット ゾーンおよびローカル イントラネット ゾーンで ActiveX コントロールおよびアクティブ スクリプトをブロックするように設定後、信頼する Web サイトを Internet Explorer の信頼済みサイト ゾーンに追加できます。これにより、信頼されていない Web サイトからの攻撃を防ぎながら、現在とまったく同じ様に、信頼する Web サイトを引き続き使用できます。マイクロソフトは信頼できる Web サイトのみを [信頼済み] サイト ゾーンに追加することを推奨します。

これを行うためには、次のステップを実行します。

① Internet Explorer で [ツール] をクリックし、[インターネット オプション] をクリックします。次に [セキュリティ] タブをクリックします。

② [Web コンテンツのゾーンを選択してセキュリティのレベルを設定する] で、[信頼済みサイト] をクリックし、次に [サイト] をクリックします。

③ 暗号化されたチャネルを必要としない Web サイトを追加する場合は、[このゾーンのサイトにはすべてサーバーの確認 (https:) を必要とする] チェック ボックスをクリックして、チェックを外します。

④ [次の Web サイトをゾーンに追加する] で、信頼する Web サイトの URL を入力し、次に [追加] ボタンをクリックします。

⑤ ゾーンに追加したい各 Web サイトについて、これらのステップを繰り返します。

⑥ [OK] を 2 回クリックし、変更を許可し、Internet Explorer に戻ります。

注: システムで悪質な動作が行われないと信頼できるすべてのサイトを追加します。特に追加すべき 2 つの Web サイトは *.windowsupdate.microsoft.com および *.update.microsoft.com です。これらはセキュリティ更新プログラムをホストする Web サイトで、セキュリティ更新プログラムのインストールには ActiveX コントロールが必要です。