

IE Base Tag Local Files Reading Vulnerability

分類 Other (Design Error)
 関連ツール名称
 再現性 リモート

技術解説

1) 概要

HTML タグである Base タグは HTML ファイル中で参照される 相対パスの基準を示すものである。Microsoft Internet Explorer には HTML タグである Base タグの取り扱いに問題がある。そのため、Base タグを利用することにより攻撃者にローカルファイルの中身を開示してしまう。その結果、攻撃者に重要な情報を漏洩してしまう可能性がある。

2) 原因

Base タグ中に書かれた URL の種別を明確にしていないことが原因である。そのため、Base タグ中にローカルファイルを示す URL ハンドラ "file:/// "を使用することにより、ローカルファイルの中身をアクセスが可能になり、その結果、ファイルの中身を開示してしまう。

IE Base Tag Local Files Reading Vulnerability

検証有無

結果 ○: 成功、×: 失敗、-: 未検証

OS	サービス	バージョン	結果
Windows 2000 SP2 (J)	Internet Explorer	6.0	○
上記以外の組合せ			-

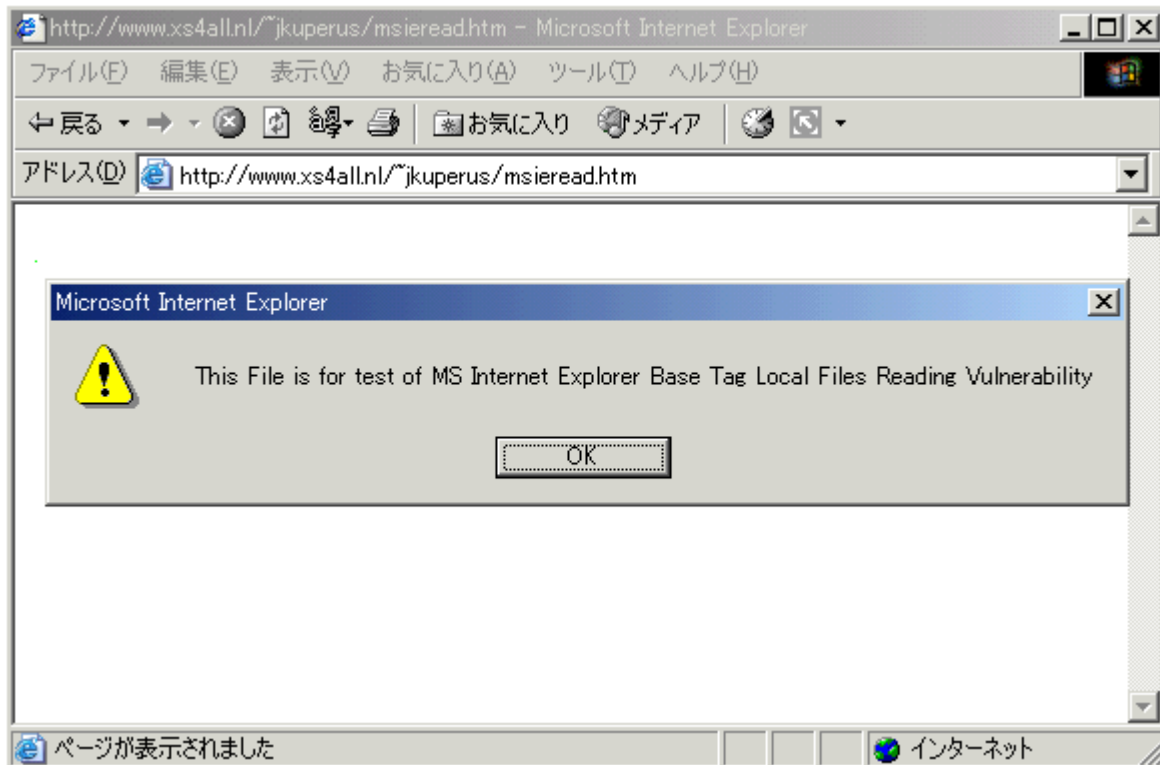
検証結果

1) 検証環境

	OS	サービス	備考
ターゲット	Windows 2000 SP2 (J)	Internet Explorer 6.0	

2) 検証結果

Internet Explorer がファイルの中身をアラートとして出力することを確認した。このことから、JavaScript 等を使用して任意のサーバにローカルファイルの中身を送信することが可能であると思われる。以下は Internet Explorer がアラートボックスをポップアップした際の様子である。



痕跡

1) ログ

イベントログには何も出力されない。

2) 痕跡

Internet Explorer のキャッシュとして Temporary Internet Files に攻撃で使用された HTML ファイルが残る。

影響

Microsoft Internet Explorer には HTML タグである Base タグの取り扱いに問題がある。そのため、Base タグを利用することにより攻撃者にローカルファイルの中身を開示してしまい、その結果、攻撃者に重要な情報を漏洩してしまう可能性がある。

影響を受けるOS、サービス

影響 ○: 脆弱性あり、×: 脆弱性なし

(2002/8/17現在)

OS	サービス	バージョン	影響	備考
Windows 全般	Internet Explorer	6.0 以前	○	

OS、サービス Windows 全般
アプリケーション Internet Explorer 6.0 以前

対策方法

1)対策

この問題に対して、ベンダーからのパッチ提供は 2002年8月28日現在、行われていない。仮対策として、ファイルの中身送信に、JavaScript や Web ページの自動更新機能が使われる事から、これらの機能を停止することが挙げられる。

2)Advisory情報

Copyright © 2002 警察庁