

Microsoft IIS のファイル拡張子処理の脆弱性に関する検証レポート

2009/12/25

NTT データ・セキュリティ株式会社

辻 伸弘

松田 和之

【概要】

Microsoft の Internet Information Server (以下 IIS) において、ファイル拡張子処理に脆弱性が発見されました。

拡張子によるアプリケーションマッピング処理を回避され、実行ファイルではない拡張子のファイルを実行ファイルとして処理される危険性があります。

想定される被害としては、アップロードできるファイル拡張子を制限している場合でも、制限を回避され、悪意あるユーザに、バックドア用の実行ファイルをアップロードされ、外部から Web サービスの実行ユーザ権限で任意のコマンドを実行される危険性があります。

今回、この Microsoft IIS の構文解析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】

Microsoft IIS

【対策案】

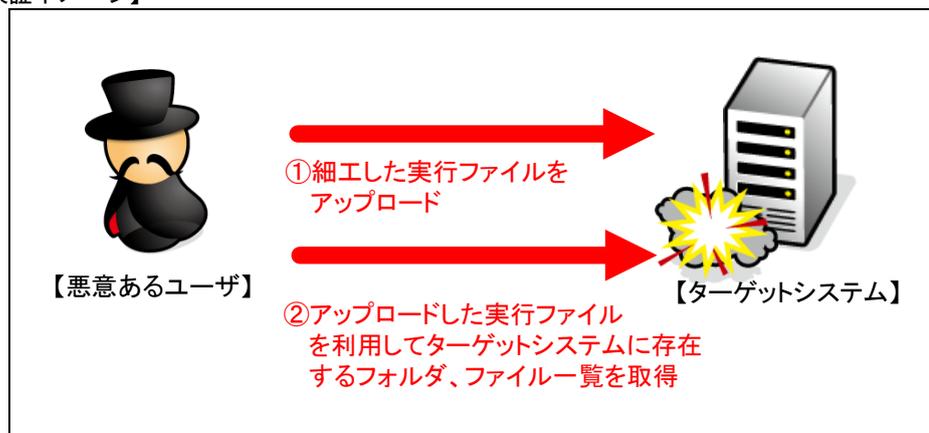
このレポート作成現在 (2009 年 12 月 25 日)、修正プログラムはリリースされておりません。

本脆弱性は、Microsoft IIS においてファイルアップロード機能を持つコンテンツが存在し、攻撃者が利用可能である場合に影響を受けます。修正プログラムリリースまでは、アップロード機能を持つコンテンツを無効にすることが推奨されます。

また、Web アプリケーションにて対応する場合は、アップロード後のファイル名をランダムにすることが推奨されます。

システム設定にて対応する場合は、アップロード先のディレクトリに実行権限を付与しないことが推奨されます。

【検証イメージ】



【検証ターゲットシステム】

Windows 2003 SP2

【検証概要】

Microsoft IIS に設置されているファイルアップロード用コンテンツにアクセスし、細工した実行ファイルをアップロードすることで、ブラウザからターゲットシステムに存在するディレクトリ、ファイル一覧の取得を試みます。

※本脆弱性は、Microsoft IIS にファイルアップロード用コンテンツが存在することが前提条件です。存在しない場合には攻撃の影響を受けることはありません。

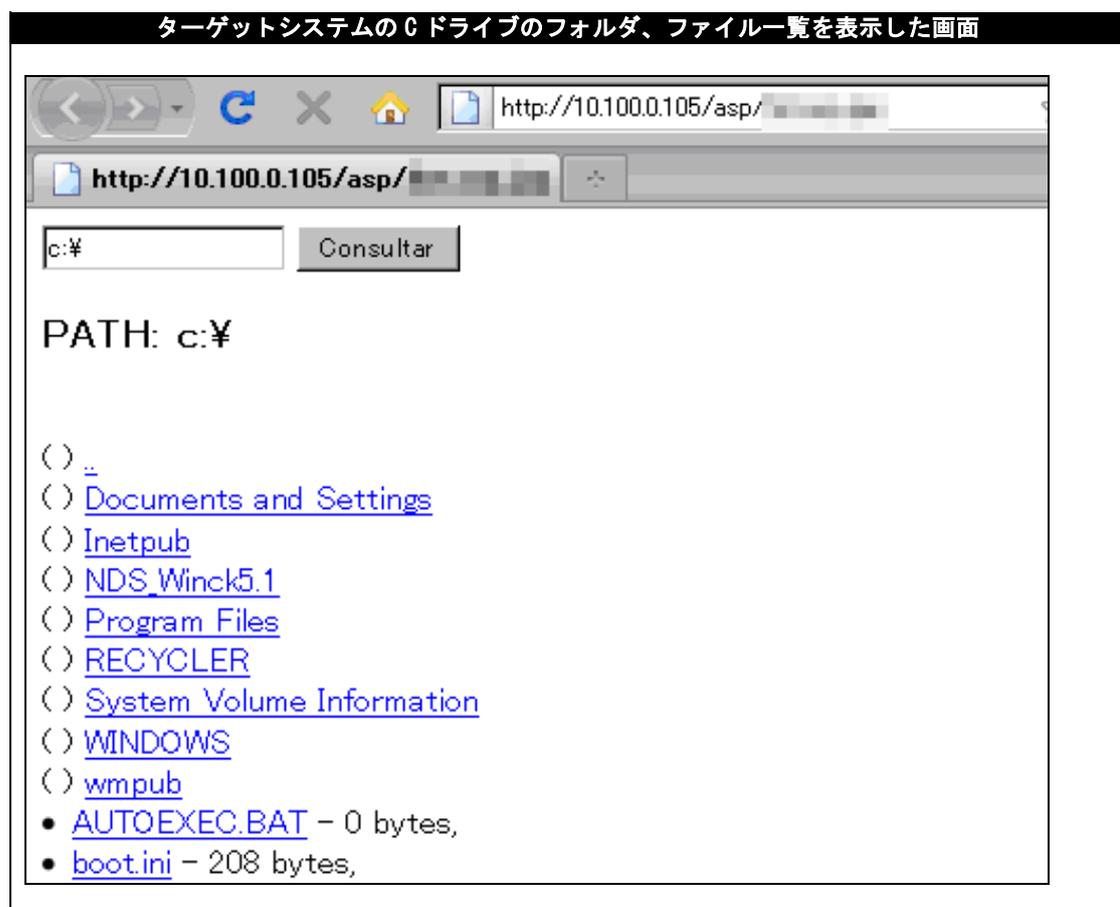
【検証結果】

下図は、実行ファイルをアップロード後、アップロードした実行ファイルを利用し、C ドライブのフォルダ、ファイル一覧を表示した画面です。

これにより、ブラウザから Web サービスの実行ユーザ権限でのフォルダ、ファイル一覧の取得に成功したと判断できます。

また、プログラムのソースコードも閲覧可能であるため、ソースコードにパスワードが書かれている場合、パスワードを取得され、なりすましに利用される危険性があります。

今回の検証では、フォルダ、ファイル一覧の取得を試みましたが、本脆弱性を利用することで、任意のコマンドが実行可能です。そのため、Web サービスの実行ユーザ権限での制御を奪取させる攻撃シナリオも想定されます。





NTTデータ・セキュリティ株式会社

* 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/>