NTTデータ・セキュリティ株式会社

Microsoft IIS の WebDAV 認証回避の脆弱性に関する検証レポート

2009/5/18
2009/5/22(更新)
2009/6/10(更新)
診断ビジネス部
辻 伸弘
松田 和之

【概要】

Microsoft の Internet Information Server 以下 IIS)において、WebDAV の Unicode 処理に脆弱性が発見されました。
本脆弱性により、Microsoft IIS での認証付きページ、及び、WebDAV での認証を回避される危険性があります。
想定される被害としては、悪意のあるユーザにより、Web サーバ上の認証付きページの認証を回避され、Web サーバに設置されているファイルすべてにアクセス可能となり、機密情報が漏洩することが挙げられます。また、WebDAV の認証を回避され、WebDAV ディレクトリ内のファイルの漏洩、改ざん、または、不正なファイルの作成を行われる危険性があります。

本脆弱性は、Microsoft IIS の WebDAV の Unicode 処理に欠陥があることに起因しています。そのため、WebDAV 機能を有効にしている Microsoft IIS では、WebDAV の脆弱性を利用され、WebDAV ディレクトリの認証に限らず、Web サーバ上で設定したすべての認証付きページに対して認証を回避されてしまいます。

今回、本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】

WebDAV 機能を有効にした Microsoft IIS 6.0
WebDAV 機能を有効にした Microsoft IIS 5.1
WebDAV 機能を有効にした Microsoft IIS 5.0

【対策案】

このレポート作成現在（2009 年 5 月 22 日)、修正プログラムはリリースされておりません。

2009 年 6 月 10 日追記：
Microsoft 社から、修正プログラム（MS09-020）がリリースされています。
十分な検証の後、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（MS09-020）の適用を行うことが推奨されます。
http://www.microsoft.com/japan/technet/security/bulletin/MS09-020.mspx

本脆弱性は、Microsoft IIS において WebDAV 機能を有効にしてい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、WebDAV 機能を一時的に無効にすることが推奨されます。

そのため、今後、修正プログラムのリリース状況を確認し、正式な修正バージョンがリリースされた際には、十分な動作検証後、速やかに適用することが推奨されます。
また、弊社のセキュリティ診断では、運用上必要なく、管理者様が把握していない状態での WebDAV の稼動がしばしば発見されます。しがたって、WebDAV が稼動していないという認識の下、Microsoft IIS を運用している場合でも、今一度、稼動の確認を行うことが推奨されます。

Microsoft IIS 6.0 における WebDAV の状態確認方法は以下のとおりです。

[管理ツール]→[インターネット インフォメーション サービス (IIS) マネージャ]→[Web サービス拡張]

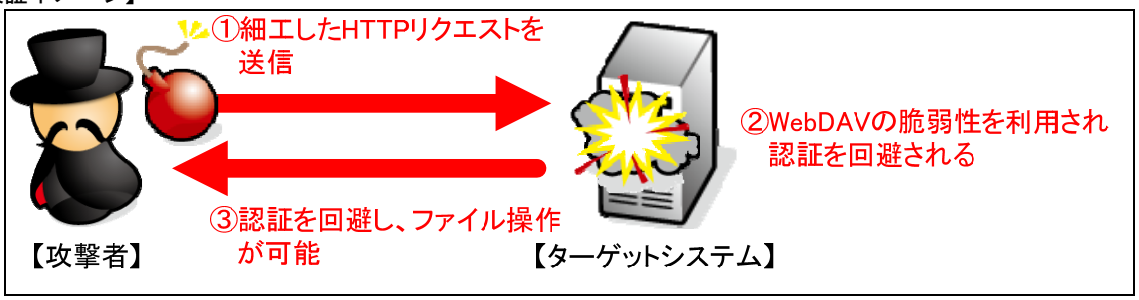
Web サービス拡張の項目「WebDAV」で現在の状態を確認することができます。

【参考サイト】

マイクロソフト セキュリティ アドバイザリ (971492)

http://www.microsoft.com/japan/technet/security/advisory/971492.mspx

【検証イメージ】



【検証ターゲットシステム】

Windows 2003 Server Standard Edition Service Pack 2 Microsoft IIS 6.0

Windows XP Professional Service Pack 3 Microsoft IIS 5.1

【検証概要】

ターゲットシステムに、細工した HTTP リクエストを送信することで、認証を回避し、ファイル操作を行います。

【検証結果】

下図は、WebDAV の Unicode 処理の脆弱性を利用し、認証を回避し、WebDAV で公開されているファイルの一覧を取得した画面です。
赤線で囲われている部分に示すように、ターゲットシステムの WebDAV ディレクトリ「webdav/」内のファイル名が取得できたことがわかります。

ターゲットシステムの WebDAV ディレクトリ内の一覧を表示した画面

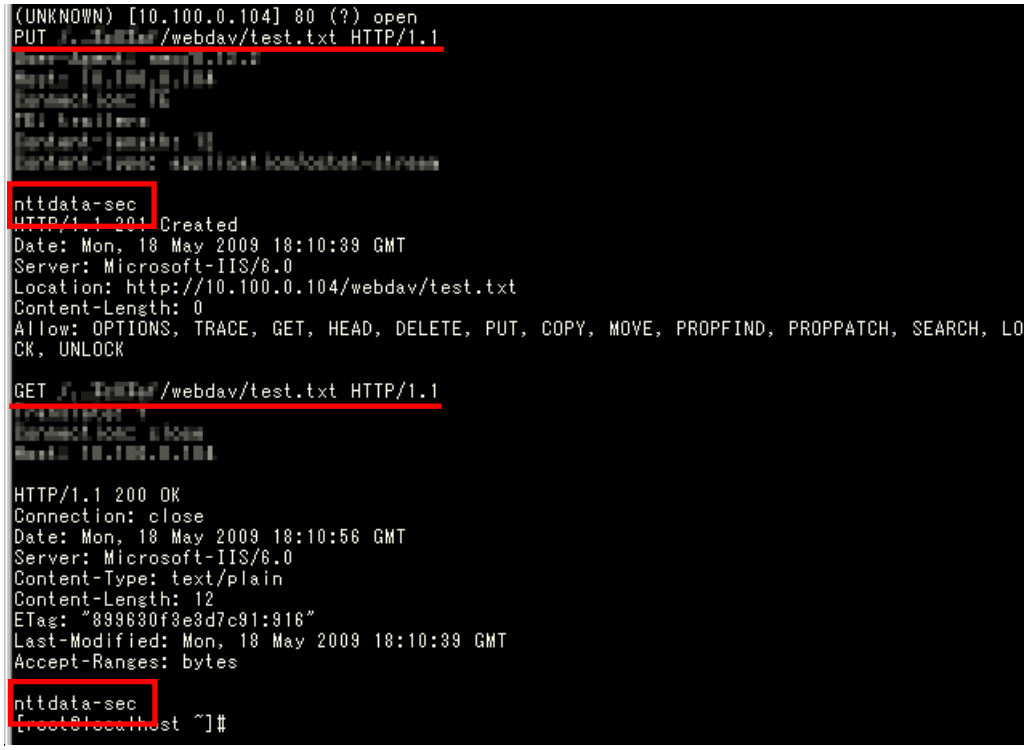
※攻撃コードを含むため、モザイク処理を施しています。

下図は、前頁で取得した情報をもとに、ファイル「secret.txt」を取得した画面です。これにより、WebDAV の認証を回避し、ファイルの取得に成功したと判断できます。

ターゲットシステムの WebDAV ディレクトリ内のファイルを読み出した画面

下図は、新規ファイル「test.txt」の書き込みを行った後、作成したファイルを取得した画面です。これにより、WebDAVの認証を回避し、ファイル操作が可能であることが証明されたと判断できます。

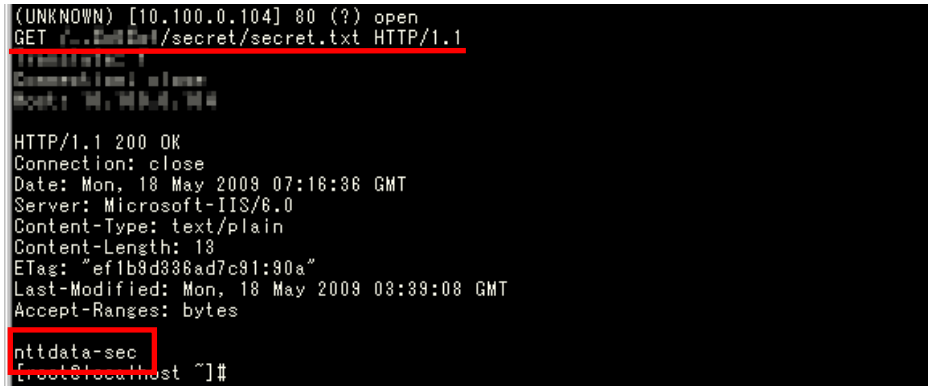
ターゲットシステムのWebDAVディレクトリ内にファイルを書き込んだ画面



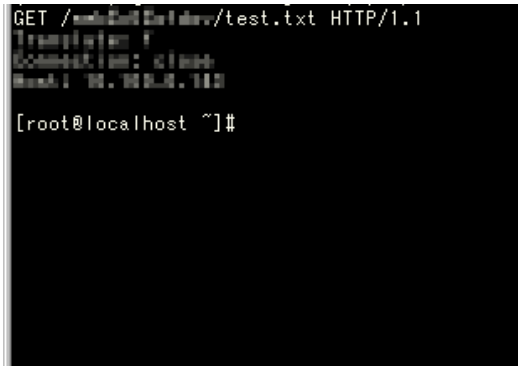
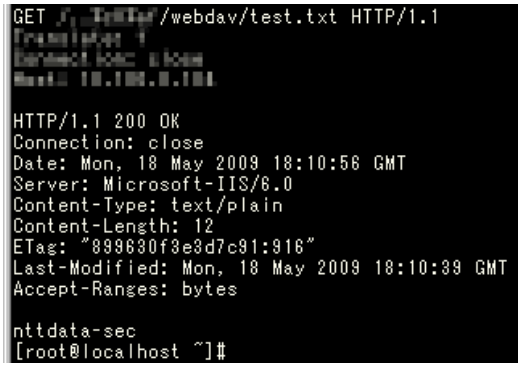
また、本脆弱性を利用することで、WebDAVの認証以外にも、Microsoft IISで設定した認証付きディレクトリの認証を回避することが可能となります。
ただし、ファイルの取得には、ファイル名を指定する必要があるため、認証付きディレクトリ内に存在するファイル名が予め分かっていることが条件となります。

下図は、本脆弱性を利用し、認証を回避し、ターゲットシステムの認証付きディレクトリ「secret/」内のファイル「secret.txt」を取得した画面です。
赤線で囲われている部分に示すように、ターゲットシステムの認証付きディレクトリ内のファイルの取得に成功したと判断できます。
この手法を利用することにより、悪意のあるユーザによって認証を回避され、Webサーバ上に設置されているファイルにアクセスされる危険性があると判断できます。

ターゲットシステムの認証付きディレクトリのファイルを読み出した画面



2009 年 6 月 10 日追記：
下図は、修正プログラム（MS09-020）適用後と適用前の検証結果画面です。以下のとおり、適用後は、認証回避ができないことが確認されました。

修正プログラム（MS09-020）適用後	修正プログラム（MS09-020）適用前
	

【対策案】
このレポート作成現在（2009 年 5 月 22 日）、修正プログラムはリリースされておりません。

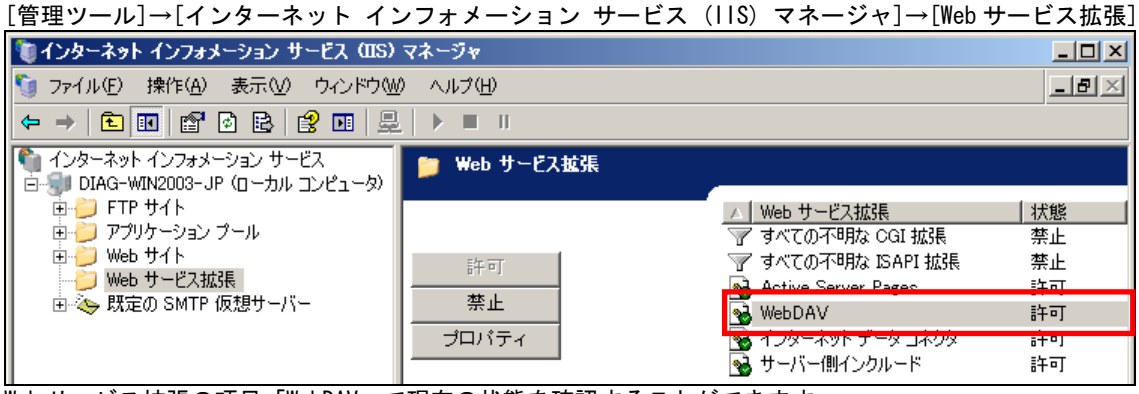
2009 年 6 月 10 日追記：
Microsoft 社から、修正プログラム（MS09-020）がリリースされています。
十分な検証の後、運用に支障をきたさないことをご確認の上、修正プログラム（MS09-020）の適用を行うことが推奨されます。
http://www.microsoft.com/japan/technet/security/bulletin/MS09-020.mspx

本脆弱性は、Microsoft IIS において WebDAV 機能を有効にしてい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、WebDAV 機能を一時的に無効にすることが推奨されます。

そのため、今後、修正プログラムのリリース状況を確認し、正式な修正バージョンがリリースされた際には、十分な動作検証後、速やかに適用することが推奨されます。
また、弊社のセキュリティ診断では、運用上必要なく、管理者様が把握していない状態での WebDAV の稼動がしばしば発見されます。しがたって、WebDAV が稼動していないという認識の下、Microsoft IIS を運用している場合でも、今一度、稼動の確認を行うことが推奨されます。

Microsoft IIS 6.0 における WebDAV の状態確認方法は以下のとおりです。

[管理ツール]→[インターネット インフォメーション サービス（IIS）マネージャ]→[Web サービス拡張]



Web サービス拡張の項目「WebDAV」で現在の状態を確認することができます。

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 (971492)
http://www.microsoft.com/japan/technet/security/advisory/971492.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/