SoftBank Technology

ソフトバンク・テクノロジー株式会社

脆弱性調査レポート

Windows Server 2003 R2 のインターネット インフォメーション サービス(IIS)6.0 における WebDAV サービスの脆弱性により、リモートから任意のコードが実行可能な脆弱性(CVE-2017-7269)に関する調査レポート

【概要】

Windows Server 2003 R2 のインターネット インフォメーション サービス(IIS)6.0 に、リモートより任意のコードが実行可能な脆弱性(CVE-2017-7269)及び、その脆弱性を利用する攻撃コードが発見されました。
本脆弱性は、IIS6.0 の拡張サービスである※WebDAV の「PROPFIND」リクエスト受信時の処理に起因するバッファオーバーフローの脆弱性で、この脆弱性を利用した攻撃が成立した場合、リモートから IIS の実行権限で任意のコードを実行される危険性があります。

本レポート作成(2017 年 4 月 3 日)時点において、本脆弱性の影響を受ける可能性がある IIS を含む Windows Sever 2003 R2 は、開発元のサポートがすでに終了 (2015 年 7 月 14 日終了)しているため、本脆弱性を修正するプログラムがリリースされない可能性が高いこと、また攻撃を成立させるためのコードが容易に入手可能であり、かつ脆弱性に対する攻撃が容易であること、加えて攻撃を受けた際にシステムへの影響が大きいことから、今回、この脆弱性(CVE-2017-7269)の再現性について検証を行いました。
※HTTP を拡張し、Web クライアントから Web サーバーのフォルダやファイルの管理を行えるようにするプロトコル

【影響を受ける可能性があるシステム】

- Windows Server 2003 R2 で IIS6.0 が動作しており、かつ WebDAV サービスを有効にしているシステム

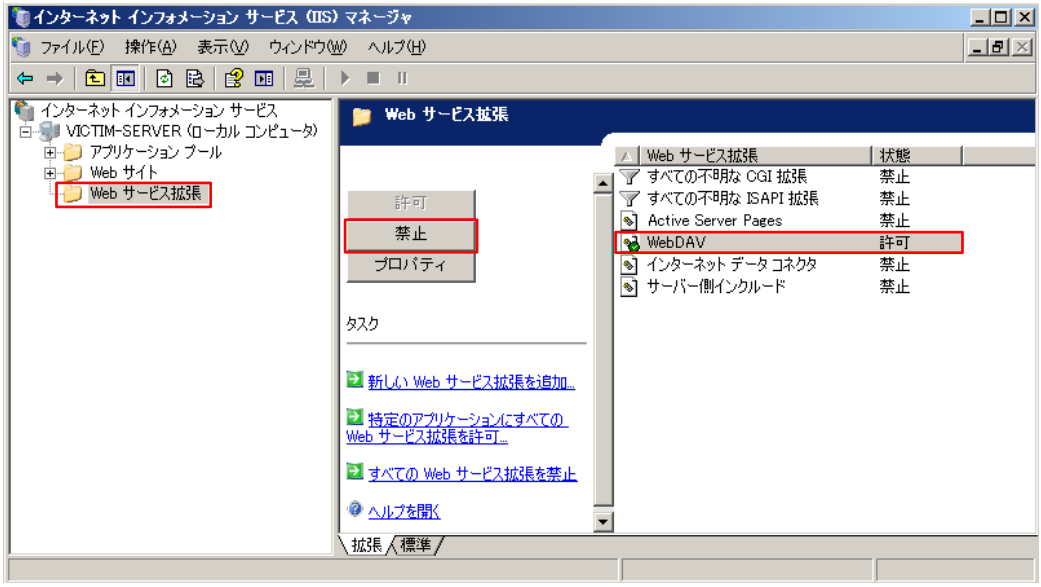
【対策案】

本脆弱性の影響を受ける可能性がある IIS を含む Windows Sever 2003 R2 は、開発元のサポートがすでに終了しているため、本脆弱性を修正するプログラムはリリースされない可能性が高いと判断できます。可能な限り迅速に現在サポート中の OS へとアップデートしてください。それまでの暫定回避策としては、WebDAV サービスを無効化、代替サービスへと変更することを推奨いたします。

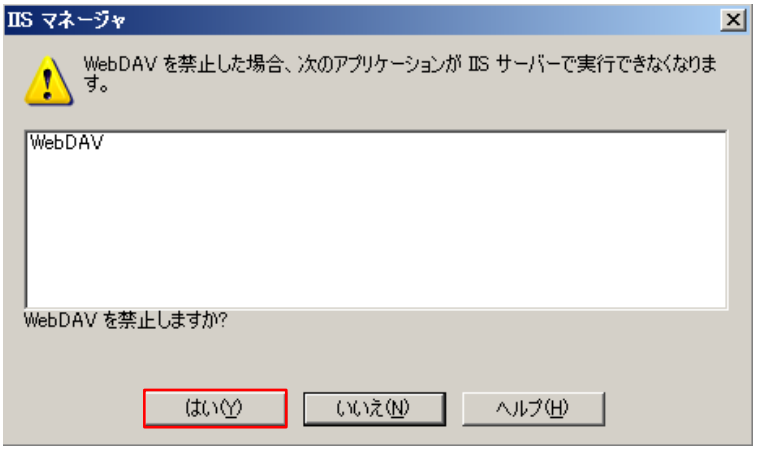
WebDAV サービスを無効化する手順は以下の通りです。

1. 管理ツールより「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」を起動します。

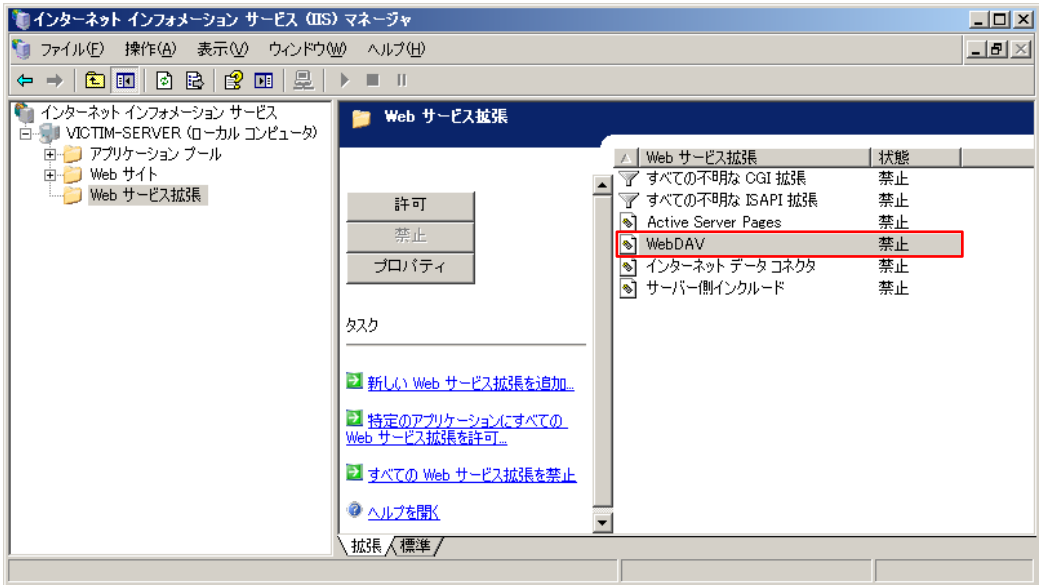
2. 左ペインのツリーを展開し、「Web サービス拡張」を選択後、右ペインにて「WebDAV」を選択し、「禁止」ボタンを押下します。



3. 下記のポップアップが表示されるので、「はい」ボタンを押下します。



4. 右ペインの「WebDAV」の状態が「禁止」になっていることを確認します。



【参考サイト】

- CVE-2017-7269
- NVD - CVE-2017-7269
- TrendLabs Security Intelligence Blog　IIS 6.0 Vulnerability Leads to Code Execution

【検証概要】

攻撃者は、ターゲットシステムで動作する IIS へ細工したリクエストを送信することにより、ターゲットシステムの脆弱性を利用して任意のコードを実行させます。

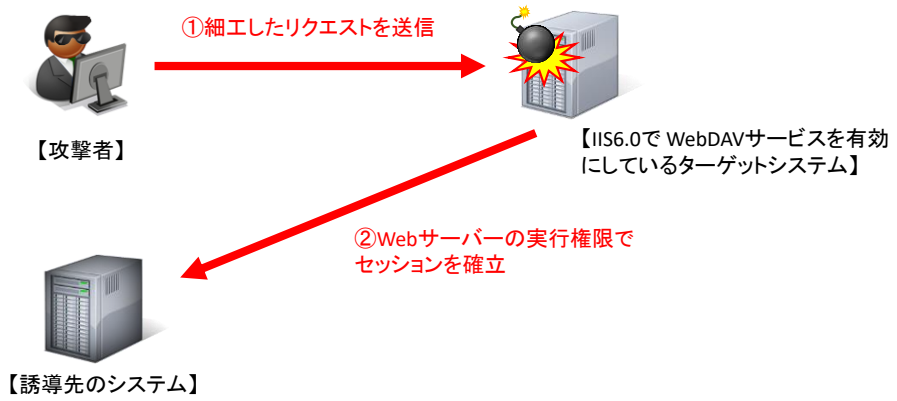
今回の検証に用いたコードは、ターゲットシステム上から特定のサーバー、ポートへコネクションを確立させるよう誘導し、システム制御を奪取するものです。これにより、リモートから IIS の実行権限でターゲットシステムが操作可能となります。

*誘導先のシステムは Linux です。

【検証ターゲットシステム】

Windows Server 2003 R2 ＋IIS6.0

【検証イメージ】

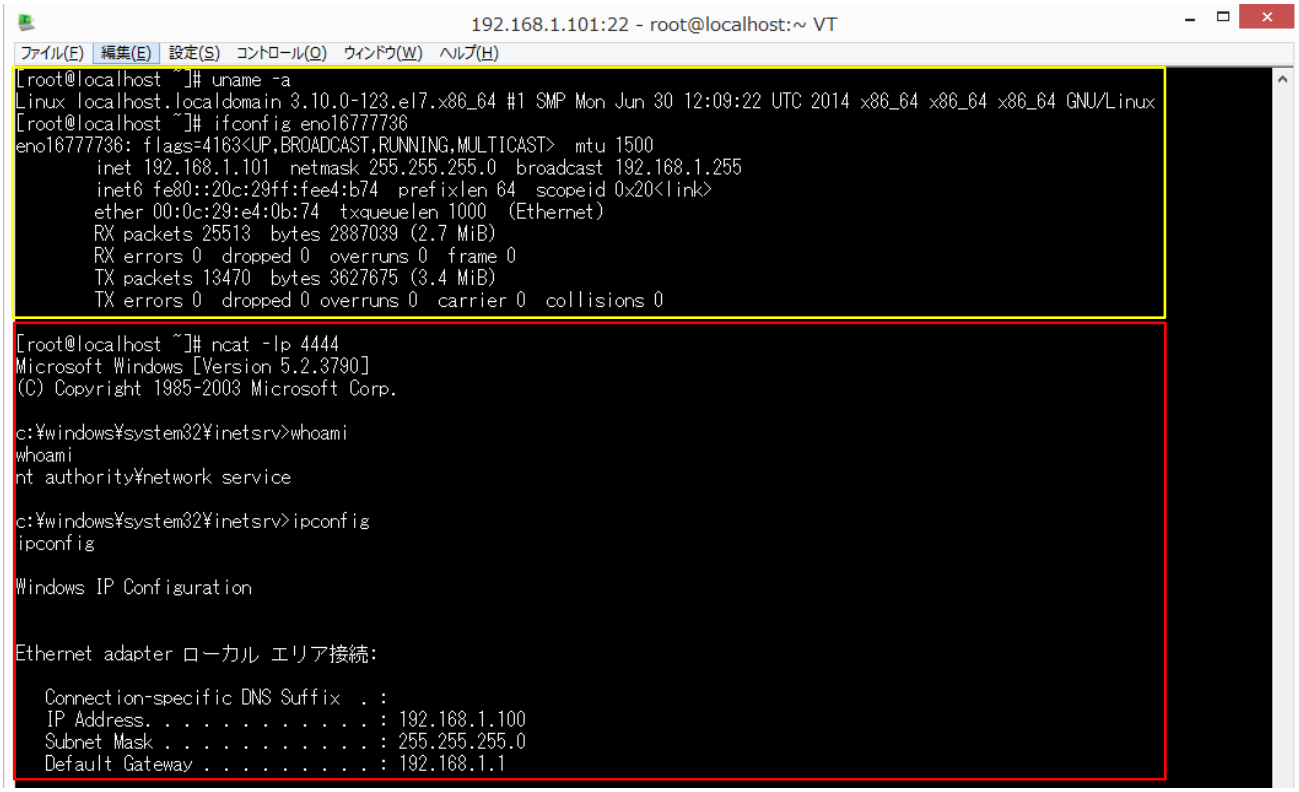

①細工したリクエストを送信
【攻撃者】
【IIS6.0で WebDAVサービスを有効にしているターゲットシステム】
②Webサーバーの実行権限でセッションを確立
【誘導先のシステム】

【検証結果】

下図は、誘導先のコンピュータ(Linux)の画面です。黄線で囲まれた部分は、誘導先のホストの情報です。

一方で、赤線で囲まれている部分は、ターゲットシステム(Windows Server 2003 R2)において、ユーザーの情報、IP アドレスの情報を表示する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で任意のコマンドを実行することに成功したと判断できます。



【更新履歴】

2017 年 4 月 3 日 ： 初版公開

ソフトバンク・テクノロジー株式会社
〒160-0022 東京都新宿区新宿 6 丁目 27 番地 30 号
新宿イーストサイドスクエア 17 階
受付時間：平日 10:00～17:00
電話 03-6892-3154
メール sbt-ipsol@tech.softbank.co.jp
URL https://www.softbanktech.jp/