

平成 15 年 3 月 28 日
警 察 庁

マイクロソフト社 Windows2000 の ntdll.dll の脆弱性に対する
Internet Information Server(IIS)5.0 を経由した攻撃の検証結果について（速報版）

1 概要

IIS 5.0 に付属している WebDAV コンポーネントが使用する ntdll.dll のうち、Windows2000 に含まれるものには、異常に長い URL を含むリクエストを受信するとバッファオーバーフローが発生する問題があり、リモートから LocalSystem 権限で任意のコマンドを実行される可能性がある。

2003 年 3 月 25 日現在、この問題を再現可能なメソッドとして、LOCK、SEARCH、PROPFIND、PROPPATCH、COPY、MKCOL、GET、PUT、HEAD、OPTIONS が報告されている。

2 原因

ntdll.dll 内の、WebDAV を利用するリクエストを処理する機能に原因がある。バッファオーバーフローが発生するプロセスが inetinfo.exe であるため、LocalSystem 権限が奪取される。

3 検証結果

COPY メソッド以外はすべて異常終了することを確認した。ただし、異常終了時のレジスタの状態等に多少の違いが見られる。

(1) LOCK、SEARCH、PROPFIND、GET、HEAD、OPTIONS メソッドの場合

URL として与える文字列にシェルコードを埋め込むなど、リモートから容易に任意のコードが実行可能であることを確認した。

(2) PROPPATCH、PUT、MKCOL メソッドの場合

異常終了するものの、任意のコードが実行できることは確認できなかった。

(3) COPY メソッドの場合

異常終了は確認できなかった。

4 痕跡

メソッドの種類にかかわらず、イベントログ(システム)に以下のようなメッセージが出力される。なお、IIS のログには何も出力されなかった。

イベントの種類: エラー イベント ソース: Service Control Manager イベント カテゴリ: なし イベント ID: 7031 説明: IIS Admin Service サービスは不正に終了しました。これは 1 回発生しています。次の修正動作が 1 ミリ秒以内に行われます: 構成された回復プログラムの実行
イベントの種類: エラー イベント ソース: Service Control Manager イベント カテゴリ: なし イベント ID: 7031 説明: Simple Mail Transport Protocol (SMTP) サービスは不正に終了しました。これは 1 回発生しています。次の修正動作が 0 ミリ秒以内に行われます: 何もしない
イベントの種類: エラー イベント ソース: Service Control Manager イベント カテゴリ: なし イベント ID: 7031 説明: World Wide Web Publishing Service サービスは不正に終了しました。これは 1 回発生しています。次の修正動作が 0 ミリ秒以内に行われます: 何もしない

5 対策

以下から入手可能なパッチを適用する。

<http://www.microsoft.com/japan/technet/security/bulletin/ms03-007.asp>

インターネット上では、IIS の WebDAV に関する機能を OFF にするなどの対策も論じられている。しかし、本脆弱性の原因が OS に含まれる DLL ファイルにあることから、IIS を介した攻撃以外の攻撃手法が今後明らかになるおそれがある。そのため、上の URL から入手したパッチを適用し、問題の DLL ファイルを更新することが望ましい。

6 参考 URL

X-FORCE Advisory:

<http://bvlive01.iss.net/issEn/delivery/xforce/alertdetail.jsp?oid=22029>

CERT Advisory CA-2003-09:

<http://www.cert.org/advisories/CA-2003-09.html>

CERT Advisory CA-2003-09(邦訳):

http://www.lac.co.jp/security/intelligence/CERT/CA-2003_09.html

SNS Spiffy Review:

<http://www.lac.co.jp/security/intelligence/SNSSpiffy/5.html>