NTTデータ・セキュリティ株式会社

Windows IIS の FTP サービスの脆弱性(CVE-2009-3023)に関する検証レポート

2009/9/2
NTT データ・セキュリティ株式会社
辻 伸弘
松田 和之

【概要】

Microsoft 社の IIS の FTP サービスに脆弱性が存在することが発見されました。この脆弱性により、リモートからコードを実行され、IIS の実行権限を制御される危険性があります。
想定される被害としては、IIS の実行権限での情報取得、改ざん、または、ワームやスパイウェアなどの悪意あるプログラムをシステム内にインストールされることが考えられます。

今回、この IIS の FTP サービスの脆弱性（CVE-2009-3023）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 Windows 2000 SP4 の Microsoft IIS5.0
Windows XP SP2、及び、SP3 の Microsoft IIS5.1
Windows XP Professional x64 Edition SP2 の Microsoft IIS6.0
Windows Server 2003 SP2 の Microsoft IIS6.0
Windows Server 2003 x64 Edition SP2 の Microsoft IIS6.0
Windows Server 2003 with SP2 for Itanium-based Systems の Microsoft IIS6.0

【対策案】

このレポート作成現在（2009 年 9 月 2 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、FTP サービスにログイン可能であり、かつ、書き込み可能であることが前提条件となります。
修正プログラムリリースまでは、以下の回避策を講じることが推奨されます。

現用のシステムでの FTP サービスの必要性の有無を確認し、不要であれば無効にすることが推奨されます。必要な場合には、アクセスする必要のある接続元を明確にし、特定の接続元からしか接続できないようアクセス制限を実施することが推奨されます。
また、匿名接続の必要性の有無を確認し、不要であれば無効にすることが推奨されます。

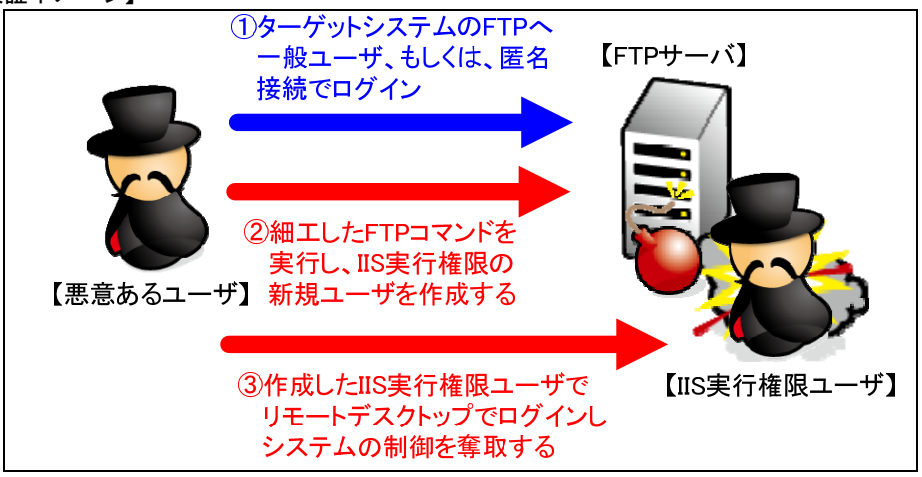
上記に加え、今一度、脆弱なパスワードが設定されている FTP サービスにログイン可能なユーザがシステム上に存在しないか確認し、存在する場合は、強固なパスワードに変更することが推奨されます。
不要なユーザが存在する場合には、直ちに削除することが推奨されます。

【参考サイト】

マイクロソフト セキュリティ アドバイザリ (975191)
http://www.microsoft.com/japan/technet/security/advisory/975191.mspx

CVE-2009-3023
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-3023

【検証イメージ】



【検証ターゲットシステム】

Windows 2000（日本語版）Service Pack 4 IIS 5.0

【検証概要】

ターゲットシステムの FTP サービスにログイン後、細工した FTP コマンドを実行することで、IIS の実行権限で任意のコマンドを実行します。
今回の検証に用いたコードは、ユーザ名「winown」、パスワード「nwoniw」のアカウントを作成するものです。
これにより、リモートからターゲットシステムが操作可能となります。

【検証結果】

下図は、攻撃前後のターゲットシステムのユーザー覧です。
右図の赤線で囲まれている部分が示すように、ターゲットシステム上に新規にユーザ「winown」が作成されており、攻撃が成功したと判断できます。

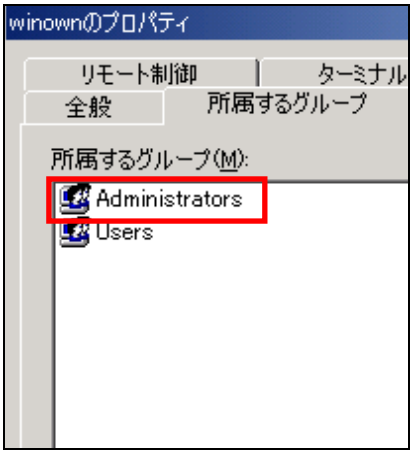
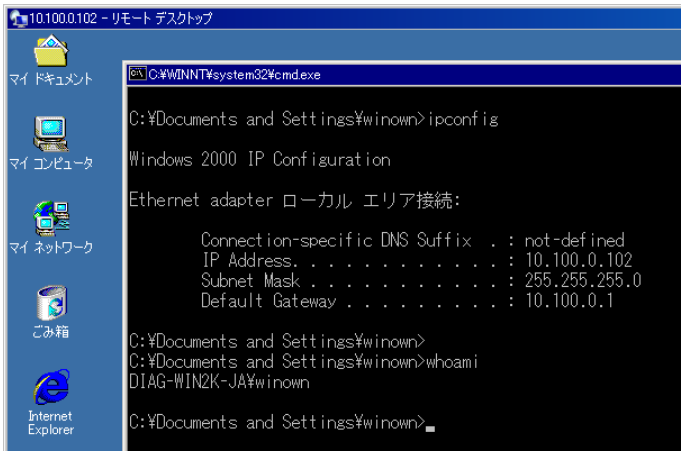
攻撃前のユーザー覧

名前	フル ネーム
Administrator	
Guest	
IUSR_DIAG-W...	インターネット ゲスト アカウン...
IWAM_DIAG-...	IIS プロセス アカウントの起動
NetShowServi...	Windows Media サービスは...
TsInternetUser	TsInternetUser

攻撃後のユーザー覧

名前	フル ネーム
Administrator	
Guest	
IUSR_DIAG-W...	インターネット ゲスト アカウン...
IWAM_DIAG-...	IIS プロセス アカウントの起動
NetShowServi...	Windows Media サービスは...
TsInternetUser	TsInternetUser
winown	

左図は、作成したユーザ「winown」が所属するグループを表示した画面、右図は、作成したユーザ「winown」、パスワード「nwoniw」でリモートデスクトップにログインした画面です。
赤枠が示すように、作成したユーザは管理者権限に所属していることから、ターゲットシステムのすべての制御の奪取に成功したと言えます。

作成したユーザの所属するグループ	作成したユーザでリモートデスクトップにログインした画面
	

【対策案】

このレポート作成現在（2009 年 9 月 2 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、FTP サービスにログイン可能であり、かつ、書き込み可能であることが前提条件となります。
修正プログラムリリースまでは、以下の回避策を講じることが推奨されます。

現用のシステムでの FTP サービスの必要性の有無を確認し、不要であれば無効にすることが推奨されます。必要な場合には、アクセスする必要のある接続元を明確にし、特定の接続元からしか接続できないようアクセス制限を実施することが推奨されます。
また、匿名接続の必要性の有無を確認し、不要であれば無効にすることが推奨されます。

上記に加え、今一度、脆弱なパスワードが設定されている FTP サービスにログイン可能なユーザがシステム上に存在しないか確認し、存在する場合は、強固なパスワードに変更することが推奨されます。
不要なユーザが存在する場合には、直ちに削除することが推奨されます。

【参考サイト】

マイクロソフト セキュリティ アドバイザリ (975191)
http://www.microsoft.com/japan/technet/security/advisory/975191.mspx

CVE-2009-3023
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-3023

＊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。

NTTデータ・セキュリティ株式会社

【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/