NTTデータ・セキュリティ株式会社

Windows カーネルの#GP トラップハンドラの脆弱性に関する検証レポート

2010/01/25
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 Windows カーネルの#GP トラップハンドラに脆弱性が存在することが発見されました。
Windows カーネルとは、デバイスやメモリ、処理時間の割り当て、エラー処理等を管理するための OS の基本機能を提供するものです。この Windows カーネルが、16 ビットアプリケーションの特定の例外を正しく処理しないことにより、今回の問題が発生します。

この脆弱性により、ローカル環境において、一般ユーザに Windows カーネルの脆弱性を利用した攻撃コードを実行され、システム権限を奪取される恐れがあります。
想定される被害としては、システム権限での情報取得、改ざんが考えられます。

今回、この Windows カーネル処理の脆弱性（CVE-2010-0232）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】

Windows 2000 SP4
Windows XP SP2、SP3
Windows Server 2003 SP2
Windows Vista SP なし、SP1、SP2
Windows Server 2008 for 32-bit Systems SP なし、SP2
Windows 7 for 32-bit Systems

【対策案】

このレポート作成現在（2010 年 1 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、16 ビットアプリケーション実行時に発生します。そのため、16 ビットのアプリケーションを実行しないように設定することも回避策となります。
なお、16 ビットのアプリケーションを実行できなくする方法については、マイクロソフトアドバイザリに提示されています。
http://www.microsoft.com/japan/technet/security/advisory/979682.mspx

また、本脆弱性はシステムに一般ユーザでログインできることが前提条件となります。そのため、今一度、脆弱なパスワードが設定されているリモート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。また、不要なユーザが存在する場合には直ちに削除するといった回避策を講じることが推奨されます。
ただし、正規のユーザによる攻撃、つまり、内部犯行を行われた場合には、上記対策は回避策とはなりません。そのため、根本的対策であるバージョンアップを講じるスケジュールを明確にすることが推奨されます。

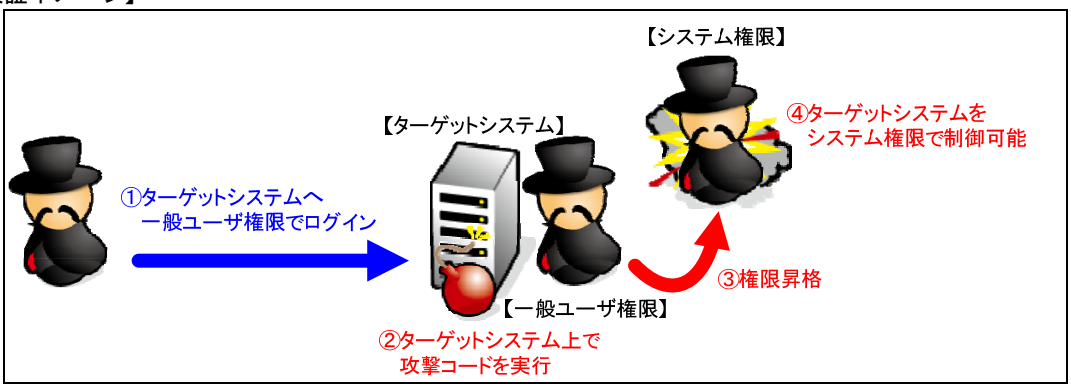
【参考サイト】

マイクロソフト セキュリティ アドバイザリ (979682)
http://www.microsoft.com/japan/technet/security/advisory/979682.mspx

CVE-2010-0232
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-0232

NTTデータ・セキュリティ株式会社

【検証イメージ】



【検証ターゲットシステム】

Windows XP SP3

【検証概要】

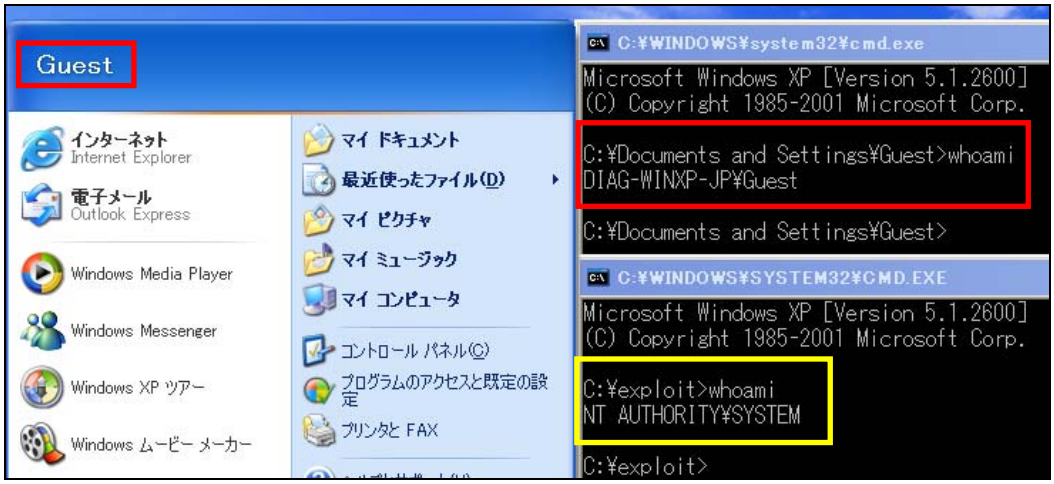
ターゲットシステムに Guest ユーザでログインし、Windows カーネル処理の脆弱性を利用した攻撃コードを実行することで、権限昇格させます。
これにより、ターゲットシステムを管理者権限で操作可能となります。

※本脆弱性は、ターゲットシステムに一般ユーザでログインできることが前提条件です。

【検証結果】

下図の赤線で囲まれている部分は、ターゲットコンピュータに Guest ユーザでログインしている情報を表しています。黄色線で囲まれている部分は、攻撃コード実行後、ターゲットシステムにおいて、システム権限「NT AUTHORITY¥SYSTEM」に昇格している情報を表しています。これにより、システム権限でのコマンド実行が可能となり、システム権限の奪取に成功したと言えます。

ターゲットシステムの管理者権限の奪取に成功した画面



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/