NTTデータ・セキュリティ株式会社

Windows カーネルの RtlQueryRegistryValues における権限昇格可能な脆弱性に関する検証レポート

2010/11/26
NTT データ・セキュリティ株式会社
辻 伸弘
小田切 秀暁

【概要】

Microsoft 社の Windows カーネルに、ローカルで攻撃可能なバッファオーバーフローの脆弱性が見つかっています。
本脆弱性により権限昇格が行われる可能性があります。脆弱性は RtlQueryRegistryValues アプリケーションプログラミングインターフェース(API)に存在します。レジストリキー作成処理が正常に処理されず、バッファオーバーフローを引き起こします。

今回、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アプリケーション】

現在のところ、影響を受ける可能性が報告されているのは次の通りです。
Windows XP, Windows Vista, Windows 7, Windows Server 2008

2010 年 11 月 24 日(米国時間)、マイクロソフト社は、当該脆弱性に関して調査を行っていると発表しています。

【対策案】

このレポート作成現在（2010 年 11 月 26 日）修正プログラムはリリースされていません。

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、修正プログラムがリリースされた際に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。

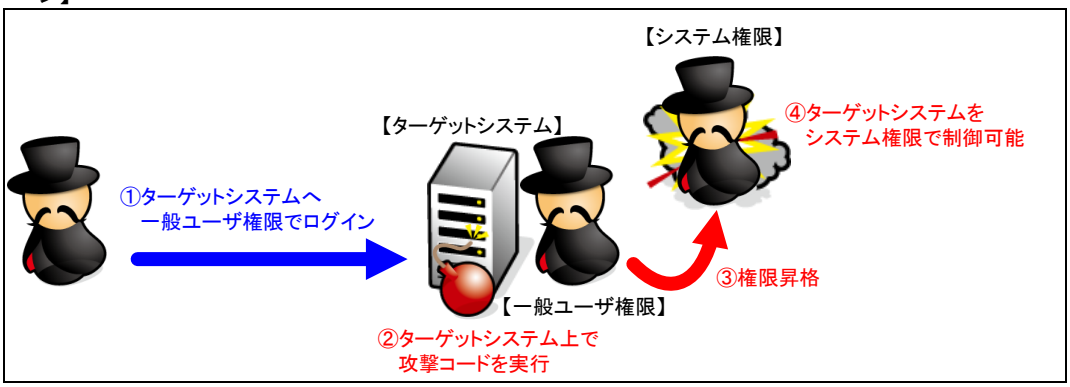
【参考サイト】

マイクロソフト社のセキュリティレスポンスセンターTwitter アカウントの投稿
http://twitter.com/msftsecresponse/status/7590788200402945

サンズ・インスティチュートのセキュリティ情報
http://isc.sans.edu/diary.html?storyid=9988

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 Vista

【検証概要】
ターゲットシステムに test 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 test 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制御の奪取に成功した画面

＊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
企画部　広報グループ
TEL:03-5425-1954
http://www.nttdata-sec.co.jp/