NTTデータ 先端技術株式会社

MySQL サーバの認証済ユーザによりシステム制御を取得する手法に関する検証レポート

2012/12/10
NTT データ先端技術株式会社
辻　伸弘
小松　徹也

【概要】

MySQL サーバに、データベース管理者ユーザによりシステムの制御を取得される手法が存在します。

データベース管理者ユーザに代表される FILE 権限（データベースを通じて任意のファイルを出力する権限）をもつユーザにて、データベースに接続します。DUMPFILE 機能を用いて、ローカルディスクにデータを生成後、Windows の MOF（Managed Object Format）を利用することで、生成したコードを実行することが可能です。
攻撃者が何らかの方法で MySQL 上の管理ユーザでのアクセス権を取得した場合、OS のシステム権限も同時に掌握されます。その結果、重要情報の改ざん、窃取されてしまうといった危険性があります。

今回、この MySQL サーバの認証済ユーザによりシステム制御を取得する手法について検証を行いました。

※脆弱性情報を取り扱う情報サイトにて、脆弱性として掲載されております。しかし、本手法については、MySQL および Windows の標準機能を利用した攻撃手法の一つとして、弊社では認識しています。

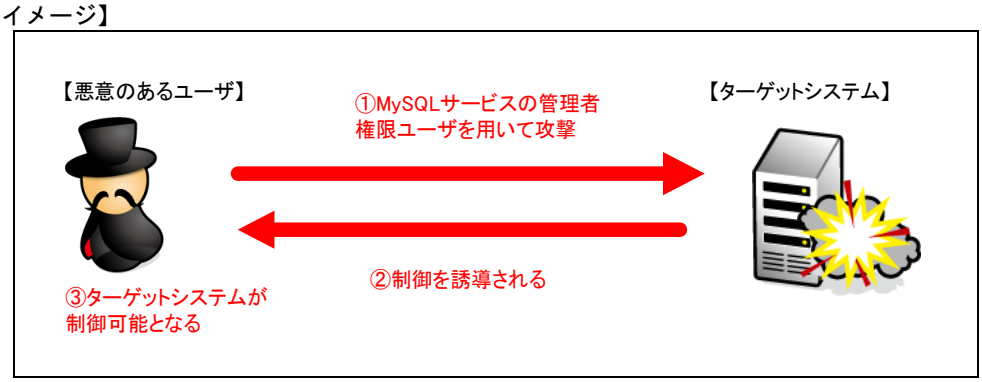
【影響を受けるとされているシステム】

- 不明（MOF を利用可能な Windows OS、FILE 権限をもつユーザを含む MySQL サーバと思われます）

【対策案】

本手法は、MySQL サーバにデータベース管理者ユーザまたは、FILE 権限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、適切なユーザに FILE 権限が与えられていることを確認し、不要な場合は権限を変更することが推奨されます。また、脆弱なパスワードが設定されているユーザが MySQL サーバ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。
加えて、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。

【検証イメージ】



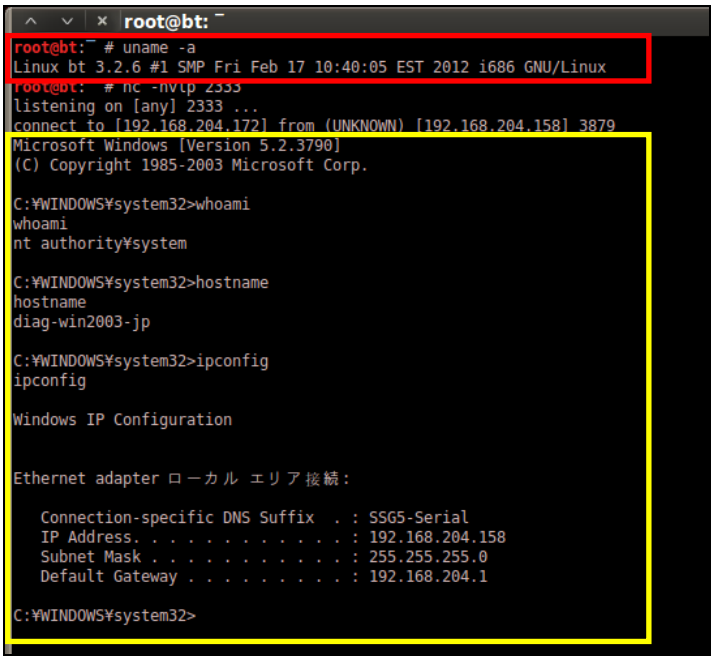
NTTデータ 先端技術株式会社

【検証ターゲットシステム】
Windows Server 2003 SP2 上の MySQL Server 5.5.28

【検証概要】
ターゲットシステム上の MySQL サーバに、データベース管理者権限ユーザで接続します。データベースの出力機能を利用し、リバースコネクトを実行するファイルをローカルに生成します。また、同様に生成した MOF ファイルから、攻撃コードを含むファイルを実行することで、制御を取得します。
今回の検証に用いた手法は、ターゲットシステム上から特定のサーバ、ポートへコネクションを確立させるよう誘導し、システムの制御を奪取するものです。
これにより、リモートからターゲットシステムを操作可能となります。
＊誘導先のシステムは BackTrack R3 です。

【検証結果】
下図の赤線で囲まれている部分の示すように、誘導先のコンピュータ（BackTrack）のコンソール上にターゲットシステム（Windows Server 2003）のプロンプトが表示されています。
黄線で囲まれている部分の示すように、ターゲットシステムにおいて、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の制御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。

【お問合せ先】
NTT データ先端技術株式会社
セキュリティ事業部
TEL:03-5859-5422
http://security.intellilink.co.jp