NTTデータ・セキュリティ株式会社

Linux Kernel の vmsplice システムコールの脆弱性に関する検証レポート

2008/2/18
NTT データ・セキュリティ株式会社
辻 伸弘
松田 和之

【概要】

Linux Kernel の vmsplice システムコール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、ローカル環境において、一般ユーザに vmsplice システムコールの脆弱性を利用した攻撃コードを実行され、一般ユーザから管理者権限へと昇格される恐れがあります。
想定される被害としては、管理者権限での情報取得、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システム】

Linux Kernel 2.6.17 から 2.6.24.1
＊ 上記システムは、すべて影響を受けるとされています。

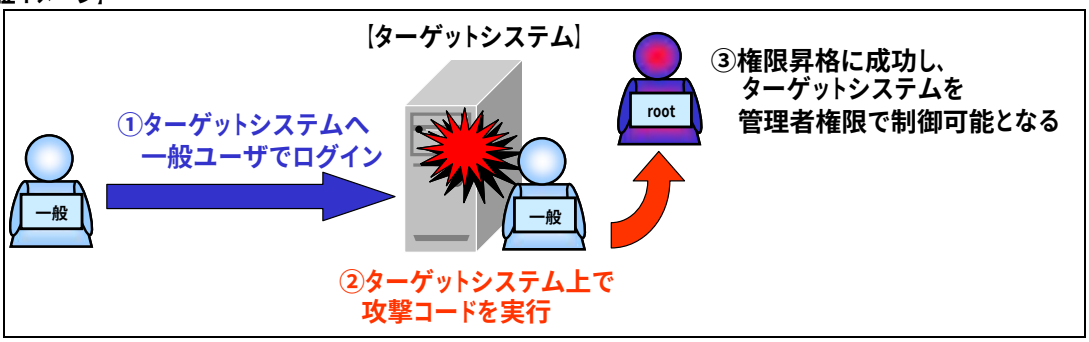
【対策案】

Linux カーネル 2.6.24.2 へアップデートすることが推奨されます。
http://www.kernel.org/

【参考サイト】

iSEC Security Research
http://www.isec.pl/vulnerabilities/isec-0026-vmsplice_to_kernel.txt

【検証イメージ】



【検証ターゲットシステム】

Linux Kernel 2.6.17 から 2.6.24.1

【検証概要】

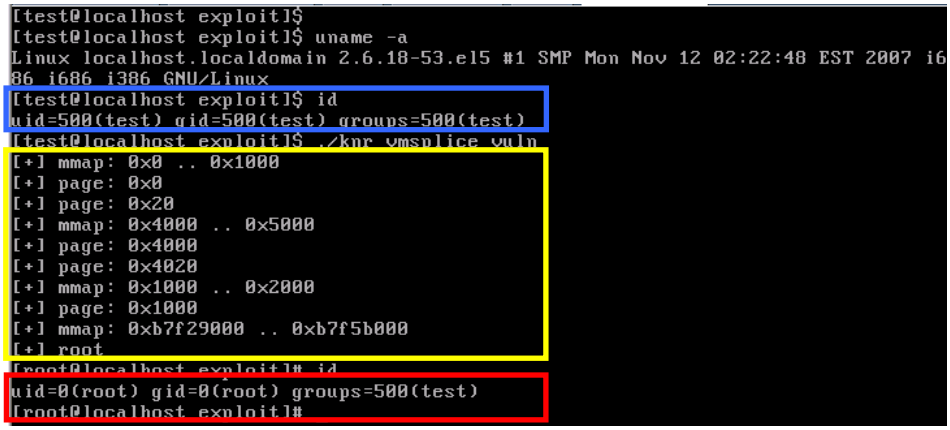
ターゲットシステムに一般ユーザでログインし、vmsplice システムコールの脆弱性を利用した攻撃コードを実行することで、権限昇格を試みます。

＊ この脆弱性は、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です。

【検証結果】

下図の青線で囲まれている部分は、ターゲットコンピュータに「test」というユーザ名の一般ユーザで権限情報を「id」コマンドで確認した結果を表しております。
そして、黄線で囲まれている部分は、攻撃コードの実行を行った部分です。
その後、赤線で囲まれている部分で「test」ユーザでのログイン後と同様に「id」コマンドにより権限情報を確認しています。
コマンドの結果において、「uid」が「test」から「root」へ変化していること、そして、プロンプトが「$」が「#」に変わっていることから、ターゲットシステム上で一般ユーザ権限から管理者権限への昇格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



【対策案】

Linux カーネル 2.6.24.2 へアップデートすることが推奨されます。
http://www.kernel.org/

【参考サイト】

iSEC Security Research
http://www.isec.pl/vulnerabilities/isec-0026-vmsplice_to_kernel.txt

【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/