NTTデータ・セキュリティ株式会社

Linux Kernel の truncate 関数、及び、ftruncate 関数の脆弱性に関する検証レポート

2008/10/31
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 が使用する truncate 関数、及び、ftruncate 関数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 truncate 関数、及び、ftruncate 関数の脆弱性を利用した攻撃コードを実行され、管理者権限グループを奪取される恐れがあります。
想定される被害としては、管理者グループ権限での情報取得、改ざんが考えられます。

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 2.6.22 未満のバージョン

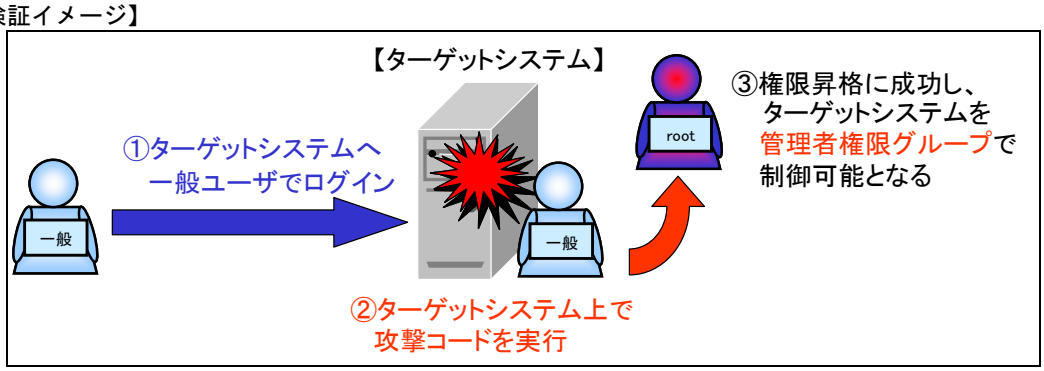
【対策案】

Linux カーネル 2.6.22 以上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】

CVE-2008-4210
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-4210

【検証イメージ】



【検証ターゲットシステム】

Red Hat Enterprise Linux Server release 5
Linux Kernel 2.6.18-8.el5

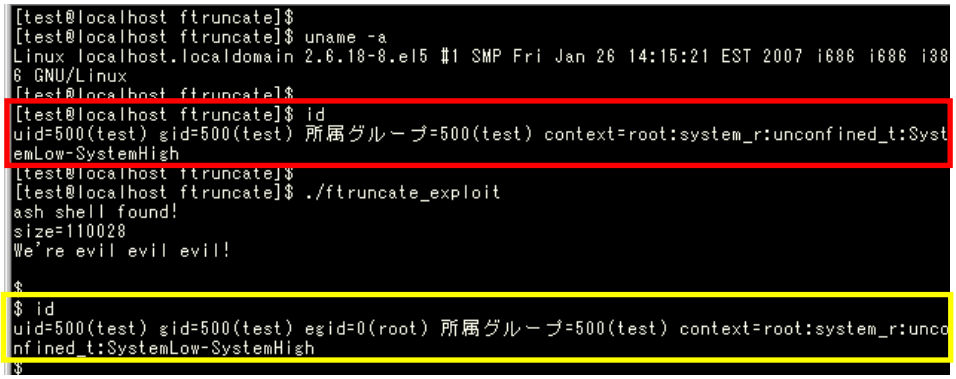
【検証概要】

ターゲットシステムに一般ユーザでログインし、ftruncate 関数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、ローカルからターゲットシステムを管理者権限グループで操作可能となります。
＊ 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】

下図の赤線で囲まれている部分は、ターゲットコンピュータに一般ユーザでログインしている情報を表しております。
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、管理者権限グループ「egid=0(root)」に昇格している情報を表しております。

ターゲットシステムの管理者権限グループの奪取に成功した画面



【対策案】

Linux カーネル 2.6.22 以上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】

CVE-2008-4210
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-4210

＊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/