NTTデータ･セキュリティ株式会社

Linux Kernel の sock_sendpage 関数の脆弱性(CVE-2009-2692)に関する検証レポート

2009/8/20
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 sock_sendpage 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 sock_sendpage 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、管理者権限での情報取得、改ざんが考えられます。

今回、sock_sendpage 関数の脆弱性（CVE-2009-2692）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 2.4.37.5 より前のバージョンを利用しているシステム
Linux Kernel 2.6.30.5 より前のバージョンを利用しているシステム
Linux Kernel 2.6.31-rc6 より前のバージョンを利用しているシステム

【対策案】

修正プログラム（Linux Kernel 2.4.37.5、2.6.30.5、2.6.31-rc6）がリリースされています。
充分な検証の後、運用に支障をきたさないことをご確認の上、修正プログラムの適用を行うことが推奨されます。

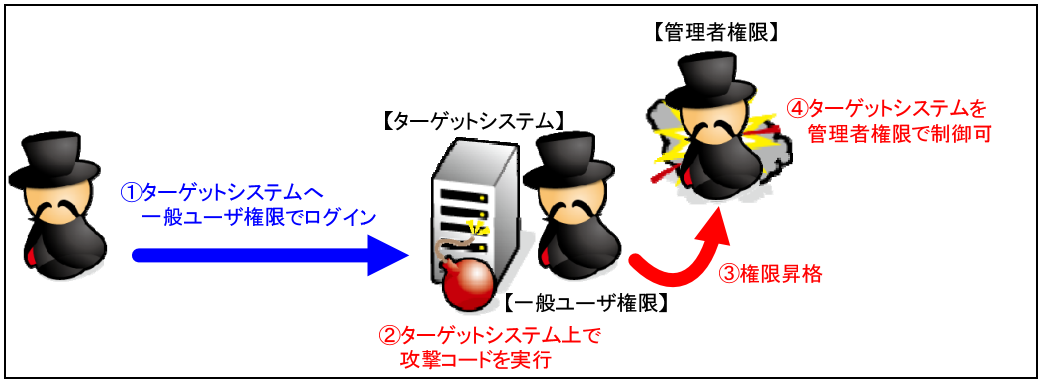
The Linux Kernel Archives
http://www.kernel.org/

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です。そのため、運用上、上記対策を実施できない場合には、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、正規のログインユーザによる攻撃、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】

CVE-2009-2692
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-2692

【検証イメージ】



NTTデータ・セキュリティ株式会社

【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

Debian GNU/Linu 5.0.2
Linux Kernel 2.6.26-2-686

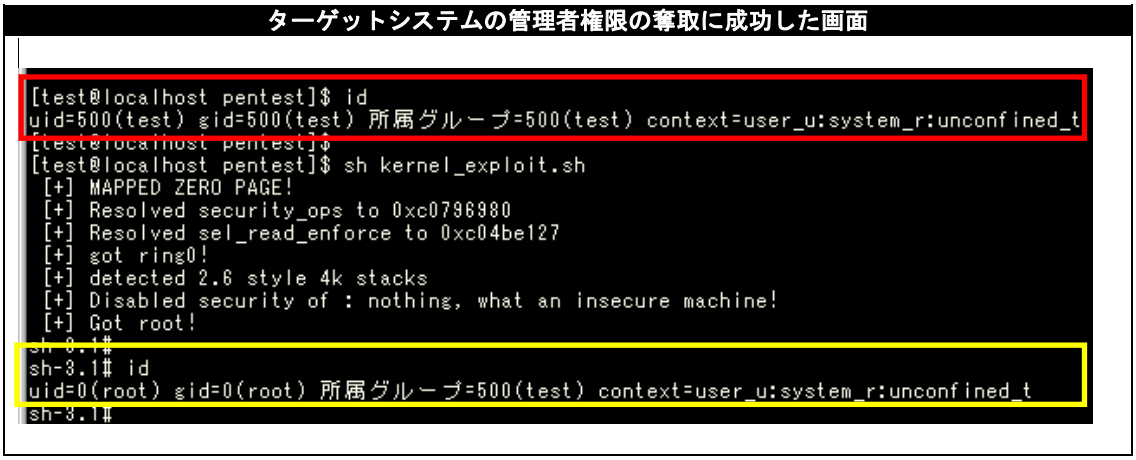
【検証概要】

ターゲットシステムに一般ユーザでログインし、**sock_sendpage** 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、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。
** 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、管理者権限「**uid=0(root)**」に昇格している情報を表しています。

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】

修正プログラム（**Linux Kernel 2.4.37.5、2.6.30.5、2.6.31-rc6**）がリリースされています。
充分な検証の後、運用に支障をきたさないことをご確認の上、修正プログラムの適用を行うことが推奨されます。

The Linux Kernel Archives
http://www.kernel.org/

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です。そのため、運用上、上記対策を実施できない場合には、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、正規のログインユーザによる攻撃、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】

CVE-2009-2692
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-2692

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
営業企画部
TEL:03-5425-1954
http://www.nttdata-sec.co.jp/