NTTデータ先端技術株式会社

複数ベンダの telnetd の libtelnet/encrypt.c における任意のコードを実行可能な脆弱性（CVE-2011-4862)に関する検証レポート

2012/1/17
NTT データ先端技術株式会社
辻　伸弘
小松　徹也

【概要】

複数ベンダの telnetd の libtelnet/encrypt.c に任意のコードが実行可能な脆弱性(CVE-2011-4862)が存在することが発見されました。この脆弱性は、libtelnet/encrypt.c 内の処理において長い暗号鍵を適切に処理しないことが起因しています。

この脆弱性により、認証前に細工した暗号鍵（注 1）を送信することで、telnetd の実行ユーザ権限（通常は root ユーザ）と同じ権限が奪取される危険性があります。

今回、複数ベンダの telnetd の libtelnet/encrypt.c における任意のコードを実行可能な脆弱性の再現性について検証を行いました。

（注 1）
Telnet にはデータストリームを暗号化する機能があります。

【影響を受けるとされているアプリケーション】

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。

- Debian Project: Debian GNU/Linux 5.0.1, 5.0.7, 6.0, 6.0.1, 6.0.2
- FreeBSD Project: FreeBSD 7, 7.4, 7.3, 8, 8.2, 8.1, 8.2
- GNU Project: Inetutils 1_8-205-g0db09b4 未満のバージョン
- Mandriva SA: 2011, 2010.1, MES5
- MIT krb5 krb5-1.8 未満のバージョン
- RedHat:
  Enterprise Linux Desktop 5, 6
  Enterprise Linux HPC Node 6
  Enterprise Linux Server 6
  Enterprise Linux Server AUS 6.2
  Enterprise Linux Server EUS 6.0
  Enterprise Linux Server EUS 6.1
  Enterprise Linux Server EUS 6.2
  Enterprise Linux Workstation 6
  Desktop Workstation 5
  Desktop 4
  Enterprise Linux 5
  Enterprise Linux AS/ES/WS 4 Enterprise Linux Long life 5.3, 5.6
  Enterprise Linux ELS 3Enterprise Linux EUS 5.6.z
  Fedora 15, 16

【対策案】

Telnet サービスの必要性を確認し、不要であればサービスを停止していただくことを推奨いたします。運用上、必要である場合は、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。この脆弱性は、認証前に利用することが可能なものですので、Telnet へ接続可能なアクセス元が適切に制限されているかという点についても確認していただきアクセス制御設定を見直すことも併せて推奨いたします。

また、Telnet は暗号化を行うオプションが利用可能ですが、そちらのオプションを用いていない場合は通信が暗号化されず、ネットワーク盗聴に対して脆弱です。そちらに根本的に対処するため可能であれば SSH などのデフォルトで通信が暗号化されるサービスへの変更もご検討いただくことも推奨されます。

【参考サイト】

CVE-2011-4862
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-4862

FreeBSD-SA-11:08.telnetd: telnetd code execution vulnerability
http://security.freebsd.org/advisories/FreeBSD-SA-11:08.telnetd.asc

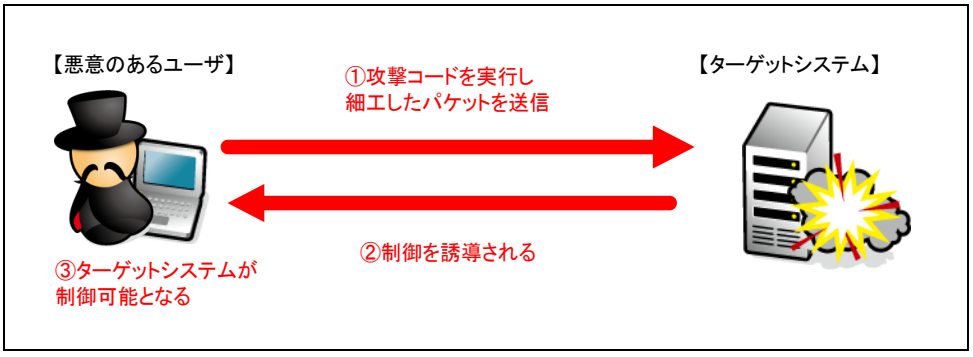
MIT krb5 Security Advisory 2011-008
http://web.mit.edu/kerberos/www/advisories/MITKRB5-SA-2011-008.txt

Debian セキュリティ勧告
http://www.debian.org/security/2011/dsa-2372
http://www.debian.org/security/2011/dsa-2373
http://www.debian.org/security/2011/dsa-2375

RedHat セキュリティアップデート
http://rhn.redhat.com/errata/RHSA-2011-1851.html
http://rhn.redhat.com/errata/RHSA-2011-1852.html
http://rhn.redhat.com/errata/RHSA-2011-1854.html

Mandriva： MDVSA-2011:195
http://www.mandriva.com/en/support/security/advisories/?name=MDVSA-2011:195

【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】
①FreeBSD 8.2 上の telnetd
②Debian 6.0.2 上の telnetd

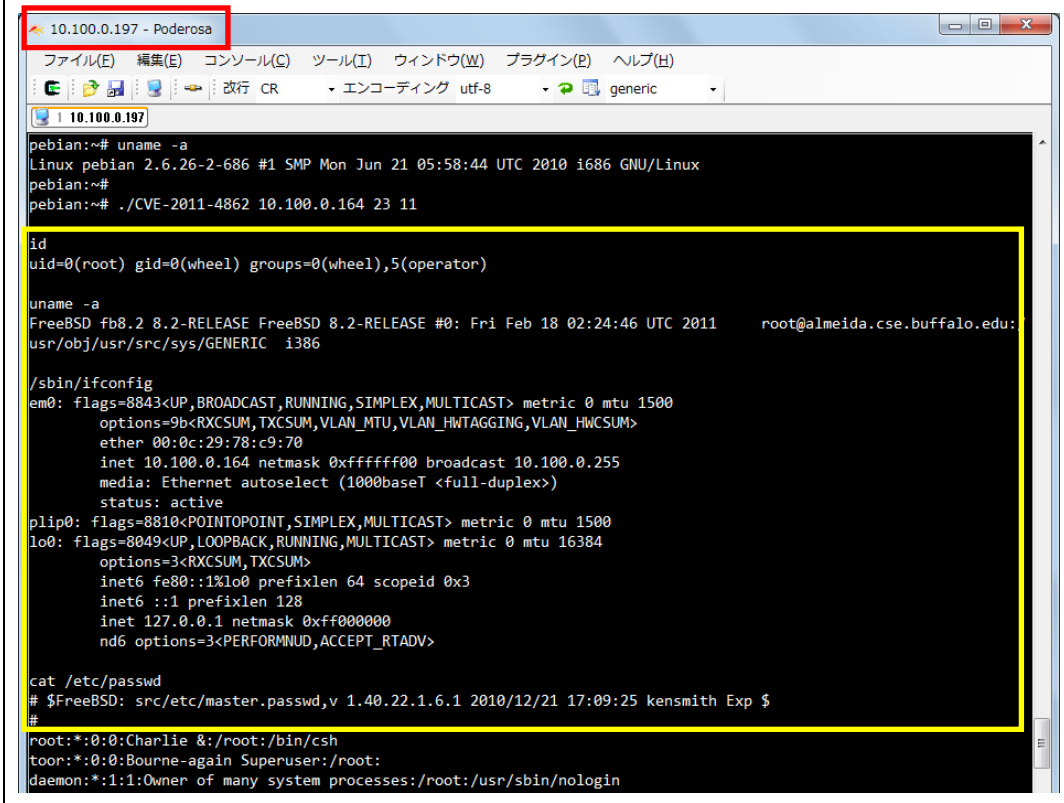
本検証では、環境の異なる 2 種類の OS に対して検証しております。項番は、後述している検証結果に対応しています。

【検証概要】
ターゲットシステムに、細工した暗号鍵を送信することで任意のコードを実行させます。
今回の検証に用いたコードは、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。
＊検証ターゲット①の誘導先のシステムは Debian 5.05 です。また、検証ターゲット②の誘導先のシステムは FreeBSD 8.2 です。

【検証結果】

①FreeBSD 上の telnetd の制御誘導
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（Debian）のコンソール上にターゲットシステム（FreeBSD）の情報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



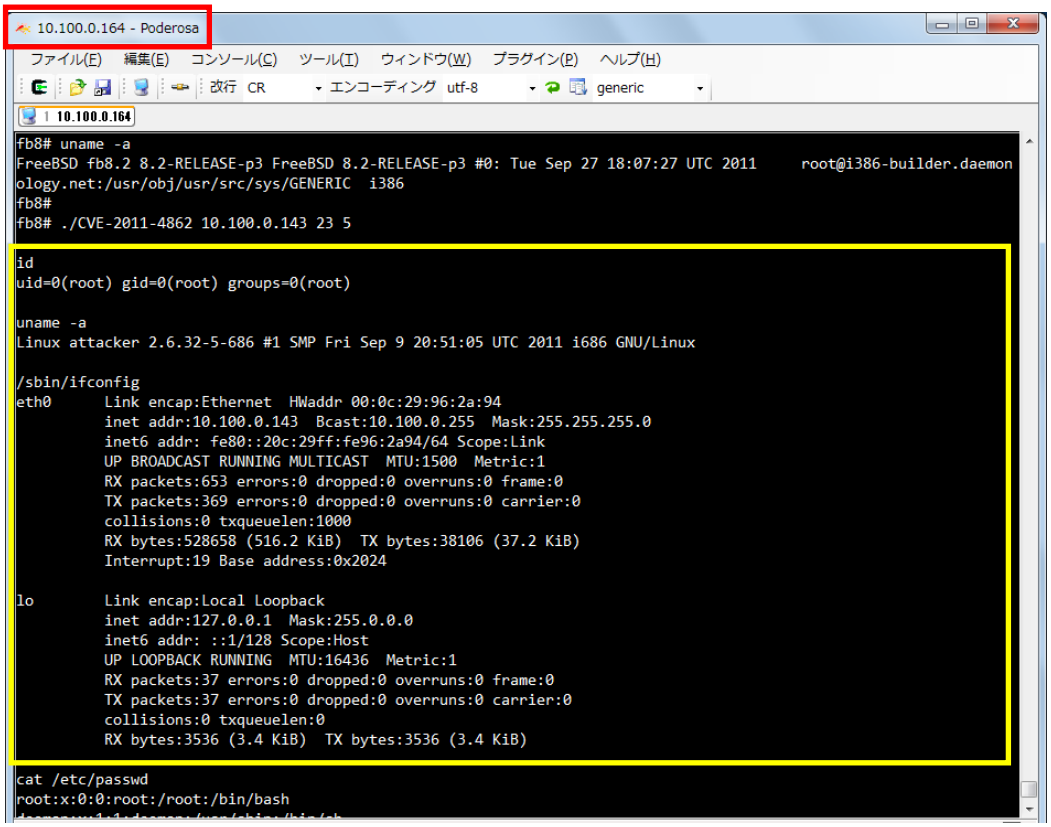
NTTデータ先端技術株式会社

②Debian 上の telnetd の制御誘導

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（FreeBSD）のコンソール上にターゲットシステム（Debian）の情報が表示されています。

①と同様に、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　営業担当　営業企画グループ
TEL：03-5425-1954
http://security.intellilink.co.jp/