NTTデータ 先端技術株式会社

Tectia SSH Server の処理の不備により認証を回避される脆弱性に関する検証レポート

2012/12/5
NTT データ先端技術株式会社
辻 伸弘
泉田 幸宏

【概要】

SSH Communications の Tectia SSH Server に、認証を回避される脆弱性が発見されました。
本脆弱性はパスワード認証を利用している場合、ユーザが自身のパスワード変更するための機能である SSH USERAUTH CHANGE REQUEST に問題があるため、パスワード変更要求処理を誤動作させることで認証を回避し、パスワードを用いることなくログインすることが可能となります。

【影響を受けるとされているシステム】

- SSH Tectia Server 6.0.4 から 6.0.20
- SSH Tectia Server 6.1.0 から 6.1.12
- SSH Tectia Server 6.2.0 から 6.2.5
- SSH Tectia Server 6.3.0 から 6.3.2

【対策案】

SSH Communications 社より、この脆弱性を修正するバージョンがリリースされています。
当該脆弱性が修正されたバージョンにアップデートしていただくことを推奨いたします。

- SSH Tectia Server 6.3.3
- SSH Tectia Server 6.1.13
- SSH Tectia Server 6.0.20 (HP-UX PA-RISC 2012/12/5 リリース予定)
- SSH Tectia Server 6.2.6 (2012/12/5 リリース予定)

また、SSH Communications 社より、パスワード認証を無効化する回避策が提示されております。

本回避策を実施した場合、パスワード認証が無効化されます。したがって、パスワード認証のみで運用を行っている場合は、回避策を実施する前に他の認証方法（キーボードインタラクティブ、GSSAPI、公開鍵認証）へ切り替えを行っていただく必要があります。

パスワード認証を無効化するためには、/etc/ssh2/ssh-server-config.xml ファイル中の
『 <auth-password /> 』を含む行（複数存在する場合は全て）を XML 形式でコメントアウトしていただく必要があります。コメントアウトの書式は『 <!--　--> 』です。

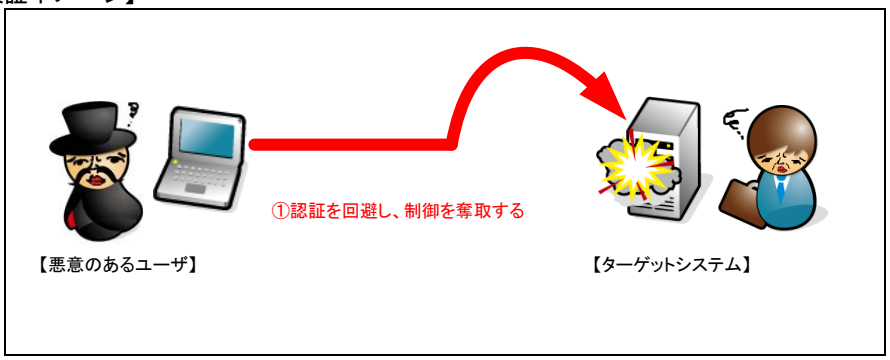
コメントアウトの例
<!-- <auth-password /> -->

【参考サイト】

SSH Communications Security | Security Advisory
http://www.ssh.com/index.php/component/content/article/531.html

「[緊急度 High/Critical] Tectia SSH Server 脆弱性の報告」
http://www.dit.co.jp/support/ssh_tectia/ssh_info_vulnerability.html

【検証イメージ】



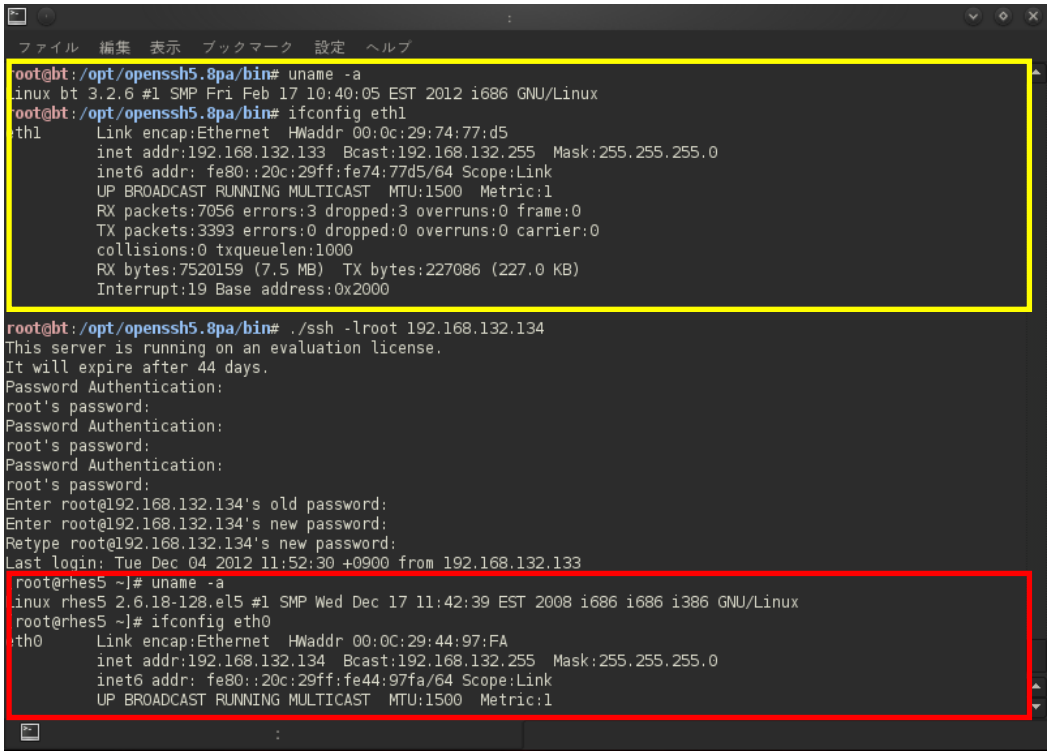
【検証ターゲットシステム】
RedHat Enterprise Linux 5.3 上の Tectia SSH Server 6.3.2.33

【検証概要】
ターゲットシステムに対して、認証リクエストを送信し、特定条件において認証を回避しログインします。今回の検証に用いた手法は、ターゲットシステム上の Tectia SSH Server に対して特別に加工した SSH で接続を行うことにより、認証を回避してログインし、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が操作可能となります。
＊ 誘導先のシステムは Ubuntu です。

【検証結果】

下図は、誘導先のコンピュータ（Ubuntu）の画面です。コンソールの黄線で囲まれている部分は、誘導先のコンピュータのホスト情報および IP アドレスです。一方で、赤線で囲まれている部分には、ターゲットシステム（RedHat Enterprise Linux 5.3）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