ソフトバンク・テクノロジー株式会社

脆弱性調査レポート

OpenSSH の脆弱性により、リモートから制限を超えるログイン試行が実行可能な脆弱性に関する調査レポート（CVE-2015-5600）

【概要】

OpenSSH でログイン処理をする際に、リモートから多数のログイン試行を実行可能な脆弱性が発見されました。
この脆弱性は、パスワード認証が有効な SSH サーバにおいて、keyboard interactive 認証の処理に欠陥があり、ログイン試行の制限時間内で任意の数の認証要求を送信することができるというものです 。
この脆弱性を利用した攻撃が成立した場合、パスワード認証のリトライ回数の制限を受けずに、パスワードの総当たり攻撃を実行することが可能です。なお、デフォルトでは認証試行を受け付ける回数（6 回）を超えるとセッションが終了する仕組みになっています。

本レポート作成（2015 年 8 月 4 日）時点において、脆弱性を修正したパッチがリリースされております（2015 年 7 月 18 日）。しかしながら、脆弱性に対する攻撃が容易であること、また攻撃を受けた際にシステムへの影響が大きいことから、今回、この脆弱性（CVE-2015-5600）の再現性について検証を行いました。

【影響を受ける可能性があるシステム】

-OpenSSH 6.9 とそれ以前のバージョン

※公開予定の OpenSSH 7.0 ではこの脆弱性に対する修正パッチが含まれる予定ですが、下記対策案を推奨いたします。

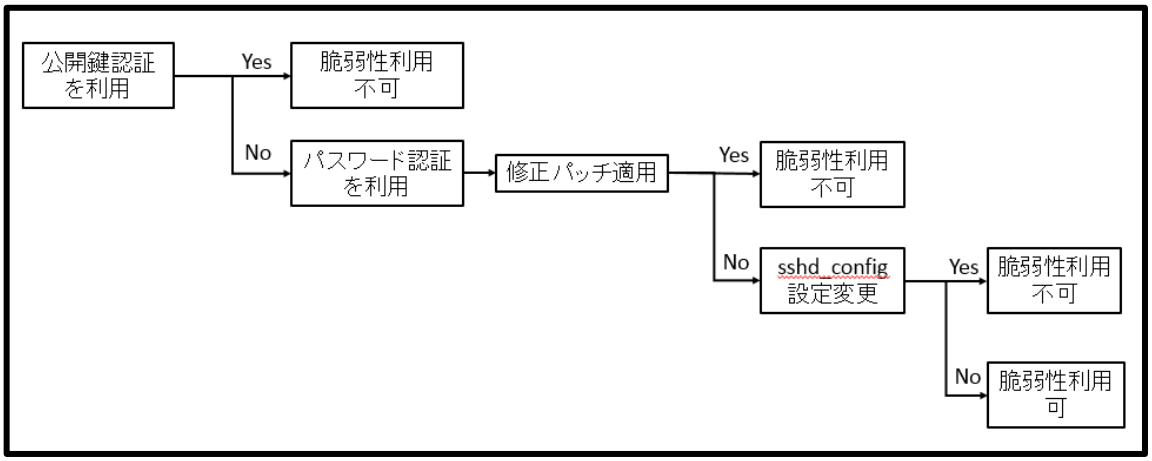
【対策案】

この脆弱性を修正するパッチがリリースされています。

当該脆弱性の修正を含む最新のパッチを適用していただくことを推奨いたします。

また、別の対策として、認証にはパスワード認証ではなく公開鍵認証を利用することも推奨いたします。

対策による脆弱性利用の可否は下図を参照してください。



パスワード認証を利用する場合、パスワードを複雑なものに設定することもあわせて推奨いたします。

また、暫定的に行う設定変更による対策としては、

/etc/ssh/sshd_config の以下の設定項目を変更することが挙げられます。

-PasswordAuthentication

-ChallengeResponseAuthentication

-UsePAM

上記 3 つの項目変更における脆弱性利用の可否については下図を参照してください。

PasswordAuthentication	ChallengeResponseAuthentication	UsePAM	脆弱性利用可否
no	no	no	否
no	no	yes	否
no	yes	no	否
no	yes	yes	可
yes	no	no	否
yes	no	yes	否
yes	yes	no	可
yes	yes	yes	可

上記全ての対策案を利用できない場合は SSH サービスをデフォルトの 22 番ポート以外でおこなうことを推奨いたします。

【参考サイト】

CVE-2015-5600

【検証概要】

ターゲットシステムに対して脆弱な設定を行った後、keyboard interactive　認証の要求と共にログイン試行を複数回受け付けるよう要求するコマンドを送信します。

その後数分間、デフォルトの認証試行を受け付ける回数（6 回）を超える認証試行が実施可能になります。

※ターゲットシステムは CentOS　です。

※/etc/ssh/sshd_config の下記設定事項は以下のとおりです。

-PasswordAuthentication　＝　yes

-ChallengeResponse Authentication = yes

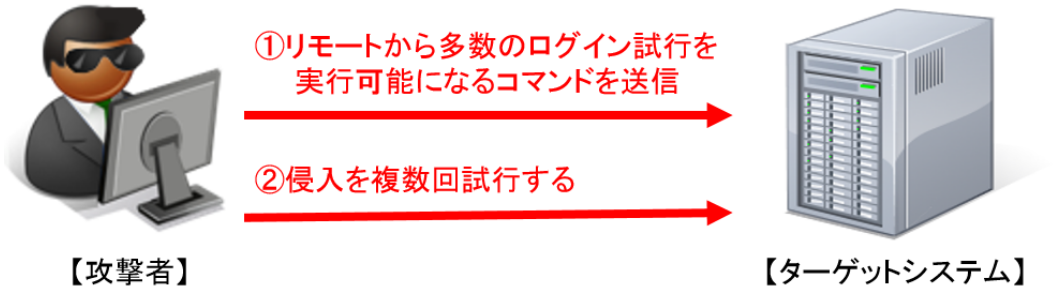
-UsePAM = yes

【検証ターゲットシステム】

CentOS linux7.0.1406

-OpenSSH のバージョン 6.4p1

【検証イメージ】



【検証結果】

下図は、リモート（攻撃者側）のコンピュータ（CentOS）の画面です。

攻撃者が細工した keyboard interactive 認証の要求を送信することで、ターゲットシステムに対してデフォルトの認証試行を受け付ける回数（6 回）を超える認証試行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に対し、デフォルトの認証試行を受け付ける回数（6 回）を超える認証試行に成功しました。

【更新履歴】

2015 年 8 月 5 日 ： /etc/ssh/sshd_config の項目変更における脆弱性利用の可否の図の誤りを修正

2015 年 8 月 4 日 ： 初版公開

ソフトバンク・テクノロジー株式会社
〒160-0022 東京都新宿区新宿 6 丁目 27 番地 30 号
新宿イーストサイドスクエア 17 階
受付時間：平日 10:00～17:00
電話 03-6892-3154
メール sbt-ipsol@tech.softbank.co.jp
URL https://www.softbanktech.jp/