-----BEGIN PGP SIGNED MESSAGE-----
Hash: SHA256

各位

JPCERT-AT-2010-0032
JPCERT/CC
2010-12-09(初版)
2010-12-15(更新)

<<< JPCERT/CC Alert 2010-12-09 >>>

不適切な設定で Asteriskを利用した場合に発生し得る不正利用に関する注意喚起

Improperly setup Asterisk may be exploited for malicious purposes

https://www.jpcert.or.jp/at/2010/at100032.txt

I. 概要

JPCERT/CC では、セキュリティ対策が不十分な状態で Asterisk を利用していたため、第三者によって意図しない国際通話を行われてしまう等の不正利用被害を受けた事例を確認しています。

※ Asterisk は、SIP サーバとして機能する IP-PBX (Intenet Protocol Private Branch eXchange) のオープンソースソフトウェアです。

攻撃者は、SIP の通信で使用される 5060/udp パケットをインターネットの広い範囲に送信し、応答した SIP サーバに対して IP 電話の発信に必要な ID、パスワードを特定するための総当たりアタックを行うと考えられます。その後、攻撃者は、特定した ID、パスワードを使用して、海外へ不正に発信します。

このため、IP-PBX のセキュリティ対策に不備があった場合、攻撃者によって、運用中の IP-PBX が不正に使用され、後日国際通話料が請求される可能性があります。

本攻撃は、IP-PBX 全体を対象に行われていると想定されますが、特にAsterisk を運用しているユーザが高額な国際通話料を請求される事例を複数確認しています。これは、Asterisk の設定を行う際に、公開されているサンプルパスワードを使用したり、容易に類推可能なユーザ名やパスワードを使用したりと、セキュリティ対策が不十分な状態で利用していたことが主な要因であると想定されます。

*** 更新: 2010年12月15日追記 **********

II. JPCERT/CC に寄せられた報告事例

JPCERT/CC は、SIP サーバに攻撃を行っていたホストに関する報告を受領しました。今回の報告で確認した SIP サーバへの攻撃では、インターネット上に公開されている攻撃ツールが使用され、ユーザ（ピア）名やパスワードを、特定するための辞書攻撃が行われていました。この攻撃に使用された辞書は、

主に数字や単語、人名で構成されていました。

[辞書に含まれている文字列の一例]
- 1桁から12桁までの数字の組み合わせ
  ※ サンプルパスワードである 1234 が含まれています。
- 単語や人名
  coffee, japan, key, account, admin, password, pass, sip, test, voip, alice, bobby, michael など
- 単純な文字列と数字の組み合わせ
  abcd123, pass1234, password1, pw1, passw0rd など

本攻撃の類似例や被害事例などの情報をお持ちでしたら、以下の Web フォーム、もしくは電子メールにて、ご報告をお願いします。

Web フォーム: https://form.jpcert.or.jp/
電子メール: info@jpcert.or.jp

****

III. 対策

運用する Asterisk を外部から不正に使用されないために、以下の対策について検討してください。(本対策は VoIP Info.jp 様の情報及び、NTT-CERT 様に提供いただいた資料をもとに記載しております)

******* ここから VoIP Info.jp 様及び NTT-CERT 様が推奨する対策 *******

1) 必要がなければ、Asterisk をインターネットに公開しない
   - ゲートウェイ (ルータ等) の内側に配置する (インターネットに直接接続しない)
   - ゲートウェイ等のファイアウォール機能で、外部から Asterisk 向けのパケットを遮断する
   - インターネットから接続する必要がある場合は、VPN 接続を利用する

2) ゲストユーザ (未設定番号) による発信を拒否する
   - ゲスト接続を許容する特別な理由がない場合は、sip.conf で、allowguest=no の設定を行う (allowguest の指定が無い場合は、デフォルトでは、ゲストユーザの発信が有効となります)

3) 総当たりアタックに対する対策を行う
   - REGISTER の際の SIP のユーザ (ピア) 名、パスワードを適切に設定する
     - パスワードを長くする。大文字、小文字、数字、記号を組み合わせ、最低でも 8 文字、可能ならば 14 文字以上の長さで設定する
     - ユーザ名を長くする (内線番号と SIP のユーザ名はイコールである必要はありません)
   - ポート番号やソース IP によるフィルタリングを行う
     - Asterisk がインストールされたサーバにおいて、通信で使用するポートのみを許可する設定を iptables 等で行う
       - 許可する IP アドレスが明確な場合は、IP アドレスの指定を行う
     - Asterisk の設定ファイルでアクセスコントロールを行う
       (例 sip.conf)

deny=0.0.0.0/0.0.0.0
permit=(発信を許可するアドレス)/255.255.255.0
- ゲートウェイ等のファイアウォール機能でフィルタリングを行う
  - 外部接続ルータやファイアウォール等で、Asterisk 向けの SIP/RTP トラフィックのみ許可する設定を行う
  - 許可する IP アドレスが明確な場合は IP アドレスの指定を行う
- ドメイン認証を使用する
  - 指定するドメイン以外の REGISTER を受け付けないようにする
    (例 sip.conf)
    domain=jpcert.or.jp
- 不要な（使用していない）ユーザは削除する
- 存在しないユーザへの返答応答を、404 から 403 に変更する
    (例 sip.conf)
    alwaysauthreject=yes
- ユーザ名、パスワードを特定するための総当たり攻撃が来ていないかログを監視する
    (Linux にインストールした場合のログファイルの例)
    /var/log/asterisk/messages
    /var/log/asterisk/cd-r-csv/Master.csv

4) 不正に外線にかけられないように対策する
- 外線プレフィックスを特殊なものにする
  - 外線発信する際に特殊なプレフィックス（番号）を付与しなければ発信できないようにする（付録 1 参照）
- 内線番号によって発信規制を行う
  - 外線発信可能な内線番号と、外線発信不可の内線番号をグループ分けする（付録 2 参照）
- 発信先の規制を行う
  - 010（国際プレフィックス）、00（中継する電話会社を指定した通話）などを利用しない場合は、特定の外線番号への発信を規制する（付録 3 参照）

※ なお、国際電話を一切利用しない場合は、利用している電話網の通信事業者にて、国際電話の利用休止をおこなうことが可能な場合がありますので、各事業者にご相談ください。

（参考）その他の推奨する対策

1) Asterisk のサービスを root 権限で起動しない
- デフォルトのインストールでは、root 権限で起動するため、一般権限ユーザ（ユーザ名の例：asterisk）でサービスを起動するように設定する

2) 管理インターフェースを使用している場合、管理用インタフェースへのアクセス制限を行う
- 遠隔からログインして CLI 機能を使用する場合は、例えば、SSH（公開鍵認証）を使用し TCP Wrapper でアクセス制限を行う
- 管理用インタフェース（AMI）を使用する場合は、manager.conf でアクセス制限の設定を行う

※ Asterisk は、複数のバージョンが存在し、今回紹介した設定例は、Asterisk 1.6.2.12-rc1 で確認しています。お使いのバージョンなどよっては、設定が異なる場合がありますので、詳細については製品のドキュメントやベンダの情報をご参照ください。

※ 付録 1 ～ 3 の設定例につきましては、以下の URL にて公開していますので、こちらも併せて、ご参照ください。

https://www.jpcert.or.jp/at/2010/at100032_sample.txt

******* ここまで VoIP Info.jp 様及び NTT-CERT 様が推奨する対策 *******

なお、利用する通信事業者によっては、本対策を行うことで接続できなくなる可能性もありますので、必要に応じて各通信事業者にご確認ください。

本対策とあわせ、JPCERT/CCでは、通話明細などで不正に利用されていないかを確認することを、お勧めします。

また、お使いの OS やソフトウエアが最新かどうかを確認し、必要に応じて、最新の状態に更新してください。他の IP-PBX をご利用の方も本対策を参考にセキュリティ対策について検討してください。

IV. 参考情報

社団法人日本インターネットプロバイダー協会
IP電話の不正利用による国際通話に関する注意喚起について
http://www.jaipa.or.jp/topics/?p=371

社団法人電気通信事業者協会
【ご注意】かけた覚えのない国際通話にご注意ください
http://www.tca.or.jp/topics/2010/1124_431.html

Asterisk SIP セキュリティ
http://voip-info.jp/index.php/Asterisk_SIP_セキュリティ

Asterisk Security Advisories
http://www.asterisk.org/security

V. 謝辞

本件の対策情報につきまして、以下の皆さまにご協力いただきました。心より感謝申し上げます。

VoIP Info.jp 様 (http://voip-info.jp/)
NTT-CERT 様 (https://www.ntt-cert.org/)

今回の件につきまして当方まで提供いただける情報がございましたら、ご連絡ください。

改訂履歴
2010-12-09 初版
2010-12-15 JPCERT/CC に寄せられた報告事例を追記

==========
一般社団法人 JPCERT コーディネーションセンター (JPCERT/CC)
MAIL: info@jpcert.or.jp
TEL: 03-3518-4600 FAX: 03-3518-4602
https://www.jpcert.or.jp/
==========
-----BEGIN PGP SIGNATURE-----

iQEVAwUBTQgtBDF9l6Rp7OBIAQgbawf/Xf5ccTZuCIOmPtyKqKz5DCcsPulXozp8
uIhp6/t7oJBL5FEFjcBjOFzzLnViju/6SL/9Kph1nTHL2LqBUeKh7yRqzQFlfwUY
x5ebHWxlQJvQ4FqdIK89HKs3fG5VPeAknLglGWXOYZvsEAo7OD9h2OrXYeUM3gK2
2KOZ2rJ17tEziG5PUwriEBopiiEq6XxgARm7eJ3B2pBBO5NHyIf+5hcL+l6Ljiiq
wM1ktLDRqbdTch+k1fOSj9OorT+LsZ8C+5fe9q/jqOC+ZolUp+9bFTC5bH4sEtIh
Ge/vRxry8Un8JuW552teYZn1Onz9fRmrOfO+/RLCCLlSHaMjo92NkA==
=HtMp
-----END PGP SIGNATURE-----