平成 30 年 3 月 28 日 作成

お客様各位

RSIT UNIX 製品における DSA 2048 鍵ファイル使用不可問題について

ネットアイキュー株式会社

RSIT UNIX 製品において、バージョン 8.0 SP2 (8.0.2.109) から DSA 2048 鍵ファイル(1024 bit 長を超える DSA 鍵ファイル) が、基本 使用出来なくなりました。従来からの鍵ファイルを継続流用しバージョンアップした場合に、接続出来なくなる重大な問題が顕在化します。

下記内容をご理解の上、該当する場合は、対応されますよう よろしくお願い致します。

記

1. 対象：

1) 対象製品/ Ver.

・RSIT UNIX Server/Client 8.0 SP2 (8.0.2.109) および それ以降

(*) RSIT Windows Server, RSIT Windows Client は影響なく使用可。

2) 対象鍵アルゴリズム

・1024 bit 長を超える DSA 鍵ファイル (特に DSA 2048 が一般的、DSA 3072 も対象)

(*) DSA 1024 は引き続き動作可能ですが、暗号強度上 RSA 2048 への置き換えを推奨。

2. 内容詳細

・SSH 接続確立時の ①"サーバ認証" と ②"ユーザ認証(公開鍵認証)" の一手段として、DSA 鍵ペアによる「署名の作成」と「署名の検証」が利用される。認証される側は"秘密鍵"により署名を作成し、認証する側は"公開鍵"によりその署名を検証する。

・今回、暗号化ライブラリの脆弱性対策(CVE-2016-0705)の影響を受け 1024 bit 長を超える DSA 鍵を使う「署名の作成」が出来なくなり下記状況となった。

1) 問題となるケース

a) 公開鍵認証用に従来 DSA 2048 鍵を使用するクライアント側を 8.0 SP2 以降に up した場合：

⇒ 接続先サーバに関わらず公開鍵認証によるユーザ認証に失敗し接続不可となる

b) サーバホスト鍵に従来 DSA 2048 鍵を使用するサーバ側を 8.0 SP2 以降に up した場合：

⇒ サーバサービス("sshd")自体は正常に稼動するが、クライアントからの接続開始直後にサーバ内対応プロセスでエラーを検知し、結果 全てのクライアントからの接続が失敗する

2) 問題とならないケース

a) 公開鍵認証用に DSA 2048 鍵を登録したサーバ側を 8.0 SP2 以降に up した場合：
(接続クライアント側は 古い RSIT UNIX 8.0 SP1 以前か RSIT Windows Client の場合)

b) 接続先サーバの DSA 2048 ホスト鍵情報を既知"hostkeys"として保存しているクライアント側を 8.0 SP2 以降に up した場合：

3. 鍵タイプ 確認方法

・生成鍵ファイル名は通常デフォルト「id_dsa_2048_xxx」となりファイル名で判断可能ですが、任意名称付与が可能なため、不確かな場合は 鍵ファイル内のコメント欄に記載された鍵タイプを cat コマンドやテキストエディタで確認します。

・RSIT 生成鍵の場合、"秘密鍵"(拡張子のない方)、"公開鍵"(".pub"拡張子) いずれでも確認可。

1) 鍵ファイルの所在

a) サーバホスト鍵 ：/etc/ssh2 ディレクトリ下 "hostkey"(秘密鍵), "hostkey.pub"(公開鍵)

b) ユーザ鍵(公開鍵認証) ：クライアント側 $HOME/.ssh2 ディレクトリ下

2) 鍵ファイル内容例

a) 秘密鍵（RSIT UNIX Server による生成例）

```
---- BEGIN SSH2 ENCRYPTED PRIVATE KEY ----
Subject: user1
Comment: "2048-bit DSA, user1@En5-RHEL5, Fri Feb 02 2018 12:18:3¥0 +0900"
          《途中省略》
---- END SSH2 ENCRYPTED PRIVATE KEY ----
```

b) 公開鍵（RSIT Windows Client による生成例）

```
---- BEGIN SSH2 PUBLIC KEY ----
Comment: "2048-bit DSA, Admin@En5-w7j64"
          《途中省略》
---- END SSH2 PUBLIC KEY ----
```

4. 対応のお願い

・対象となる DSA 2048 鍵ファイルを RSA 2048 鍵ファイルに置き換え、再設定配備頂く。

5. 補足事項

・各製品/Ver.の鍵生成仕様と DSA 鍵生成上の制限について：

1) RSIT UNIX Server/Client

a) インストール時の新規生成サーバホスト鍵

・[6.1 SP2 (6.1.2) 以降] RSA 2048。[6.1.0 以前] DSA 2048。

b) ssh-keygen コマンド

・DSA 2048 鍵生成：[8.0 SP2 (8.0.2.109) 以降] 不可。[8.0 SP1 HF3 (8.0.1.74) 以前] 可。

・デフォルト生成鍵：[6.1 SP2 (6.1.2) 以降] RSA 2048。[6.1.0 以前] DSA 2048。

2) RSIT Windows Server

a) インストール時の新規生成サーバホスト鍵

・[6.1 SP3 以降] RSA 2048。[6.1 SP2 以前] DSA 1024。

b) GUI 画面 ホスト鍵生成

・DSA 2048 鍵生成：[6.1 SP3 以降] 不可。[6.1 SP2 以前] 可。

c) ssh-keygen コマンド

・DSA 2048 鍵生成：[8.2 SP1 以降] 不可。[8.2 以前] 可。

・デフォルト生成鍵：[6.1 SP3 以降] RSA 2048。[6.1 SP2 以前] DSA 2048。

3) RSIT Windows Client

a) GUI 画面 鍵生成

・DSA 2048 鍵生成：[6.0 以降 全 Ver.] 不可。

b) ssh-keygen コマンド

・DSA 2048 鍵生成：[7.2 SP4 Update1 以降] 不可。[7.2 SP4 以前] 可。

以上