SoftBank Technology

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

Samba の脆弱性により、リモートから任意のコードが実行可能な脆弱性（CVE-2017-7494）に関する調査レポート

【概要】

書き込み可能な共有をもつ Samba に、リモートより任意のコードが実行可能な脆弱性（CVE-2017-7494）及び、その脆弱性を利用する攻撃コードが発見されました。

本脆弱性は、名前付きパイプ※を処理する際の不具合に起因する脆弱性で、この脆弱性を利用した攻撃が成立した場合、リモートから任意のコードを実行される危険性があります。なお、本脆弱性は対象の Samba に対して書き込み可能なユーザー権限を保持している場合にのみ有効な脆弱性です。

※プログラム間でファイルの読み書きが可能となるよう、データを共有する仕組み。

本レポート作成（2017 年 5 月 31 日）時点において、開発元である The Samba Team より脆弱性を修正するパッチおよび最新版がリリースされております（2017 年 5 月 24 日付）。しかしながら、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-2017-7494）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】

- バージョン 4.4.14、4.5.10 および 4.6.4 を除く Samba 3.5.0 以降のバージョン

NAS などの製品において、Samba を用いてファイルサーバー機能を実現している製品があります。使用している製品で、Samba が動作しているか、本脆弱性の影響を受けないか、また対処方法があるかを製品メーカーに確認することを推奨いたします。

現在利用している Samba のバージョンは、以下のコマンドを実行することにより確認が可能です。

smbd --version

（実行例）

```
root@debian:~# smbd --version
Version 4.5.8-Debian
```

【対策案】

The Samba Team より、この脆弱性を修正するパッチおよび最新版が公開されているため、該当パッチの適用もしくは最新版へアップデートしていただくことを推奨いたします。

【参考サイト】

- Samba - Security Announcement Archive
- Patching CVE-2017-7494 in Samba: It's the Circle of Life
- Samba にリモートからのコード実行の脆弱性(CVE-2017-7494)

【検証概要】

攻撃者は、Samba が動作するターゲットシステムの共有フォルダに悪意のある共有ライブラリをアップロード。その後に細工したリクエストを送信し、同ライブラリをロードすることにより、ターゲットシステムの脆弱性を利用して任意のコードを実行させます。

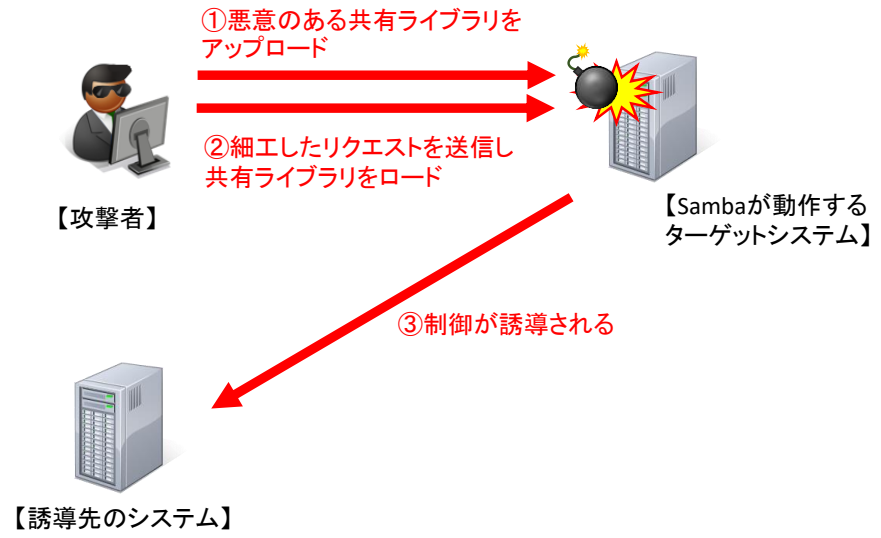
今回の検証に用いたコードは、ターゲットシステム上から特定のサーバー、ポートへコネクションを確立させるよう誘導し、システム制御を奪取するものです。これにより、リモートからターゲットシステムが操作可能となります。

*誘導先のシステムは Debian です。

【検証ターゲットシステム】

Ubuntu 15.04 + Samba 4.1.13

【検証イメージ】

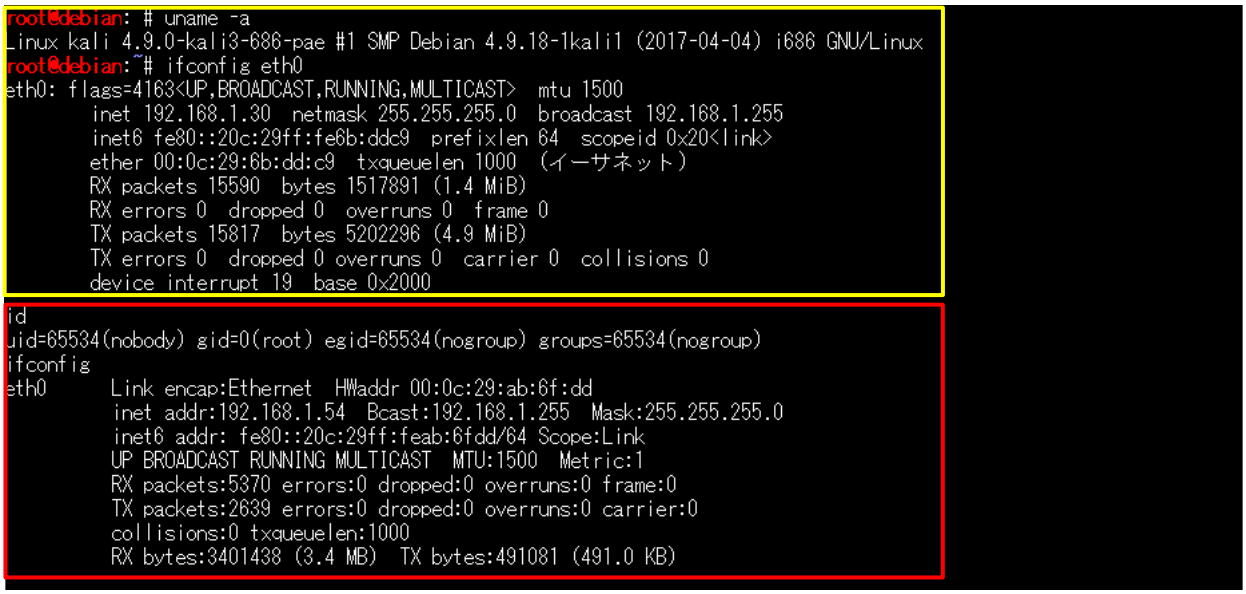


【検証結果】

下図は、誘導先のコンピュータ(Debian)の画面です。黄線で囲まれた部分は、誘導先のホストの情報です。

一方で、赤線で囲まれている部分は、ターゲットシステム(Ubuntu)において、ユーザーの情報、IP アドレスの情報を表示する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で任意のコマンドを実行することに成功したと判断できます。



【更新履歴】 2017 年 5 月 31 日 ： 初版公開

【本レポートに関するお問い合わせは下記まで】

▼報道関係者様からのお問い合わせ

ソフトバンク・テクノロジー株式会社　管理本部　経営企画部　齊藤、吉田、菅

TEL：03-6892-3063　メールアドレス：sbt-pr@tech.softbank.co.jp

▼お客様からのお問い合わせ

下記フォームよりお問い合わせください。

https://info.softbanktech.jp/public/application/add/508