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

Linux カーネルの脆弱性により、権限昇格が行える脆弱性（CVE-2014-3153）に関する調査レポート

【概要】

Linux カーネルに、システムにログイン可能な一般ユーザーが権限昇格を行える脆弱性（CVE-2014-3153）の攻撃方法が発見されました。この脆弱性は過去に Android の root 化を行う目的で利用されていた実績のある脆弱性です。この脆弱性は、kernel の futex サブシステムの処理に不備が存在しており、悪意のあるローカルユーザーが細工した futex システムコールを送信することでリングプロテクション 0 の制御を奪取することが可能です。

【上記説明の参考】

- Linux kernel futex local privilege escalation (CVE-2014-3153)
- Debian セキュリティ勧告

本レポート作成（2014 年 11 月 28 日）時点において、The Linux Kernel Archive より 2014 年 6 月 7 日に脆弱性を修正するバージョンのカーネルがリリースされていることが確認できております。しかしながら、攻撃を成立させるためのコードが容易に入手可能であり、かつ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-2014-3153）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】

- Linux Kernel 3.14.5 よりも以前のバージョン

現在利用されているシステムのカーネルバージョンは、以下のコマンドを実行することにより確認が可能です。

uname -r

```
[test@testos ~]$ uname -r
3.10.0-123.el7.x86_64
[test@testos ~]$
```

【対策案】

この脆弱性を修正するバージョンのカーネル（3.14.6）がリリースされています。

また Redhat Enterprise Linux の場合、6 系ならば kernel-2.6.32-431.20.3.el6 以降のパッケージで、7 系ならば kernel-3.10.0-123.4.2.el7 以降のパッケージでこの問題が修正されています。

当該脆弱性が修正されたカーネルにアップデートしていただくことを推奨いたします。

なお、この脆弱性を利用するためには、システムにログインできることが前提です。そのため、運用上カーネルのアップデートを実施できない場合は、システムに登録されているユーザーのパスワードを強固にしていただくこと、またシステムへのアクセス可能な経路を必要最低限に制限していただくことにより、攻撃を受ける可能性を低減することが可能です。
しかしながら、正規のユーザーによりこの脆弱性を利用された場合は、上記の対策は回避策とはなりません。よって、根本的に問題を解決していただくため、カーネルのバージョンアップを実施していただくことが推奨されます。

【参考サイト】

- CVE-2014-3153
- JVNDB-2014-002785 Linux Kernel の kernel/futex.c の futex_requeue 関数における権限を取得される脆弱性
- Kernel ChangeLog-3.14.6

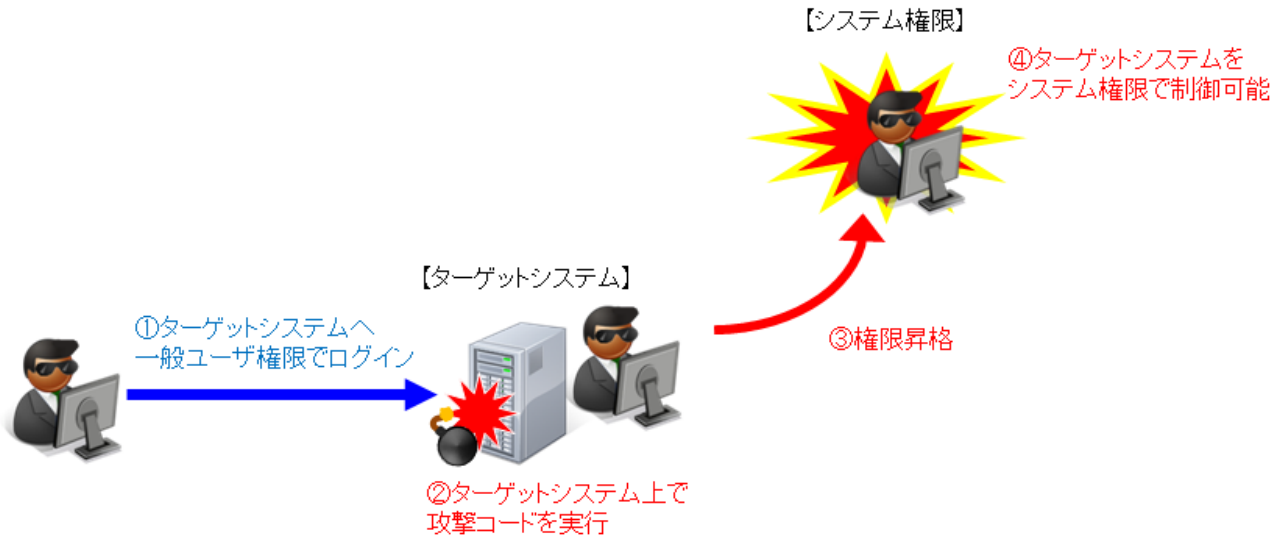
【検証概要】

脆弱性の存在するターゲットに一般ユーザーでログイン後、攻撃者が作成した細工されたコードを実行することにより権限昇格を行い、結果 root 権限を奪取するというものです。
これにより、ターゲットで全権の操作が可能となります。

【検証ターゲットシステム】

CentOS 7.0.1406

【検証イメージ】



【検証結果】

下図は、ターゲットシステム（CentOS）の画面です。黄線で囲まれている部分は、細工されたコードを実行する前のカーネル情報および一般ユーザーを示す ID 情報が表示されています。一方、赤線で囲まれている部分は、細工されたコードを実行した後の画面で、root ユーザーの ID 情報が表示されています。

これにより、ターゲットシステムで権限昇格を行うことに成功しました。

```
[test@testos ~]$ uname -a
Linux testos 3.10.0-123.el7.x86_64 #1 SMP Mon Jun 30 12:09:22 UTC 2014 x86_64 x86_64 x86_64 GNU/Linux
[test@testos ~]$
[test@testos ~]$ id
uid=1000(test) gid=1000(test) groups=1000(test)
[test@testos ~]$
[test@testos ~]$ ./exploit

[root@testos ~]#
[root@testos ~]# id
uid=0(root) gid=0(root) groups=0(root),1000(test)
[root@testos ~]#
```

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/