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-2017-6074）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-2017-6074）の攻撃方法が発見されました。

この脆弱性は Linux カーネルの※DCCP プロトコル実装において、DCCP_PKT_REQUEST の処理に問題があることから「use-after-free」の状態となり、任意のカーネルコードが実行可能となります。本脆弱性は、CONFIG_IP_DCCP オプションが有効な状態でビルドされた Linux カーネルが対象となっており、多くのディストリビューションでは同オプションはデフォルトで有効になっております。

今回、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、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、この脆弱性（CVE-2017-6074）の再現性について検証を行いました。

※DCCP（Datagram Congestion Control Protocol）は TCP や UDP と同じトランスポート層で動作するプロトコルです。

【影響を受ける可能性があるシステム】

- Linux Kernel 4.9.11 までのバージョンで CONFIG_IP_DCCP オプションが有効な状態でビルドされたシステム

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

（実行例）

```
$ uname -r
4.4.0-62-generic
$ _
```

CONFIG_IP_DCCP オプションが有効になっているかは、カーネルのコンフィグレーションファイルより確認できます。

Ubuntu16.04 の Kernel 4.4.0-62-generic では、以下のコマンドを実行することにより確認が可能です

grep /usr/src/linux-headers-4.4.0-62-generic/.config –e CONFIG_IP_DCCP

（実行例）

```
root@ubuntu:~# grep /usr/src/linux-headers-4.4.0-62-generic/.config -e CONFIG_IP_DCCP
CONFIG_IP_DCCP=m
```

CONFIG_IP_DCCP オプションが有効な場合には以下が出力されます。

```
CONFIG_IP_DCCP=m
```

CONFIG_IP_DCCP オプションが無効な場合には以下が出力されます

```
CONFIG_IP_DCCP is not set
```

【対策案】

この脆弱性を修正するパッチが公開されています。また、一部ディストリビューションからは同脆弱性が修正されたバージョンのカーネルがリリースされているため、該当パッチの適用もしくは同脆弱性が修正されたカーネルバージョン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条件となります。

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ユーザー、及び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、システムへのアクセス権を有している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。したがって、根本的に問題を解決していただくためには、カーネルのバージョンアップを実施いただくこととなりますのでアップデートを即時実施できない場合はアップデートのスケジューリングを行うことを推奨いたします。

【参考サイト】

- Linux kernel: CVE-2017-6074: DCCP double-free vulnerability (local root)
- CVE-2017-6074
- linux kernel に特権昇格の脆弱性(CVE-2017-6074)
- Use-after-free in the IPv6 implementation of the DCCP protocol in the Linux kernel - CVE-2017-6074

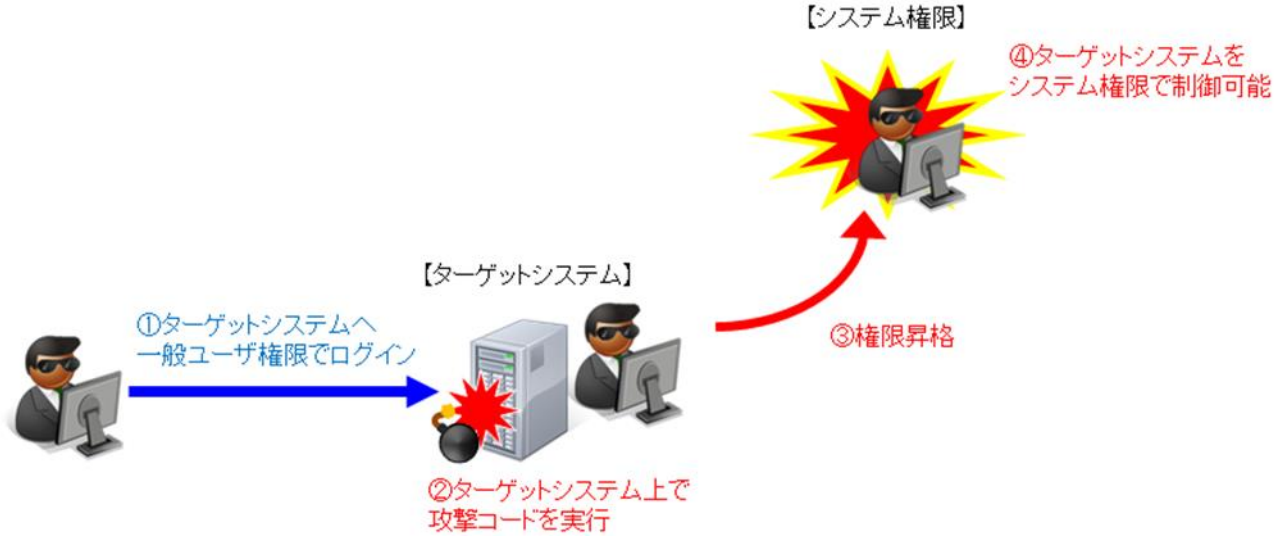
【検証概要】

脆弱性の存在するターゲットシステム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、管理者権限(root)に昇格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】

Ubuntu 16.04 + Kernel 4.4.0-62-generic

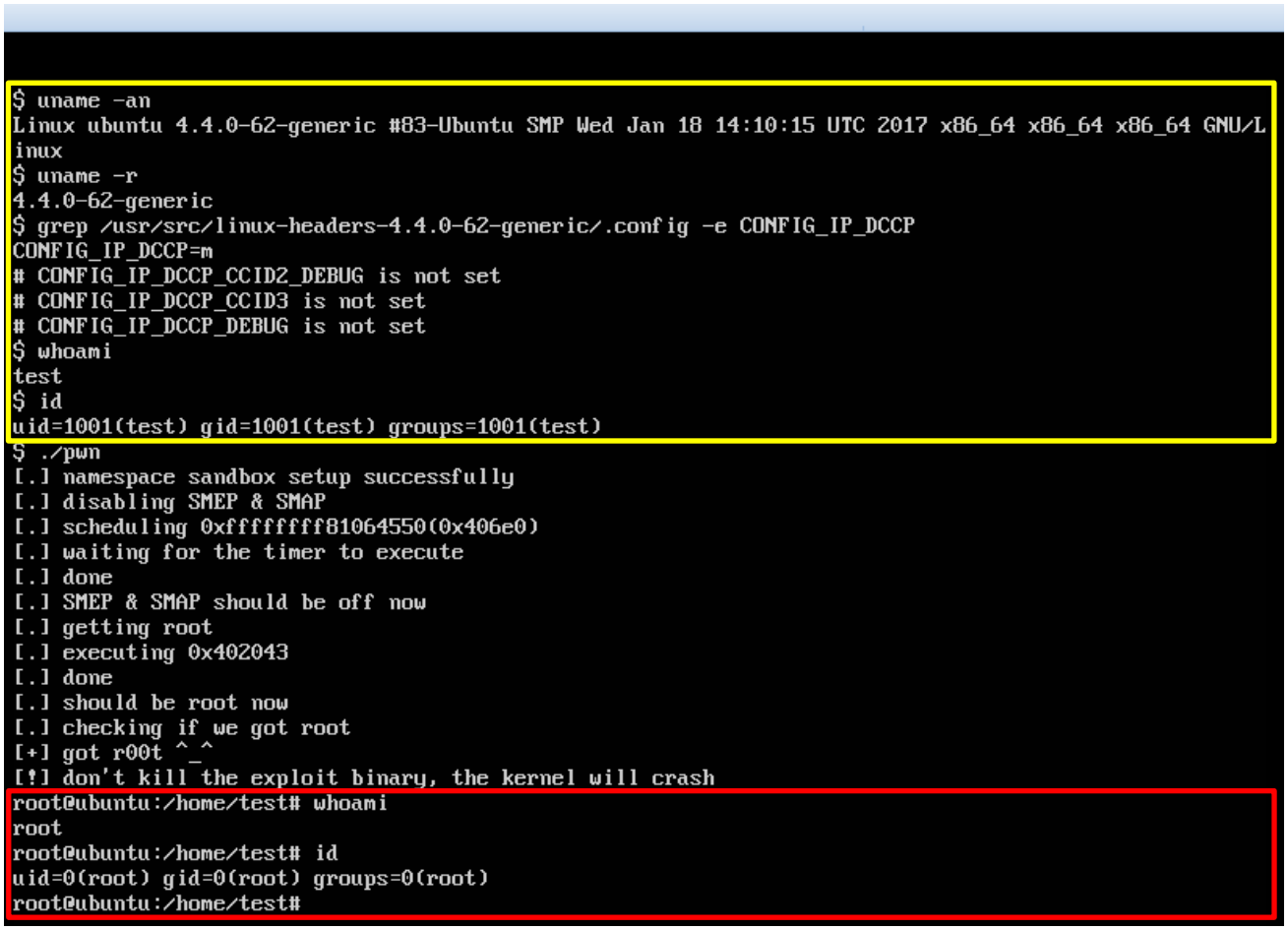
【検証イメージ】


【システム権限】
④ターゲットシステムを
システム権限で制御可能
【ターゲットシステム】
①ターゲットシステムへ
一般ユーザ権限でログイン
③権限昇格
②ターゲットシステム上で
攻撃コードを実行

【検証結果】

下図は、ターゲットシステム（Ubuntu）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状態で、管理者ユーザー（root）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たことが分かります。



【更新履歴】

2017 年 3 月 1 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/