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-2016-5195）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-2016-5195）の攻撃方法が発見されました。

この脆弱性は Linux カーネルのメモリサブシステム内の copy-on-write 機能(COW)の実装に問題があることから競合状態が発生し、ローカルの一般ユーザー権限にて、読み取り専用メモリへの書き込みが可能となります。*

そのため、一般ユーザー権限を取得した攻撃者がこの脆弱性利用した後、権限昇格を行い管理者権限を取得し、結果としてシステムを掌握することが可能です。

*この脆弱性は、copy-on-write 機能(COW)に問題があることから、「Dirty COW」と命名されています。

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、また既にこの脆弱性を利用した攻撃活動が確認されていることから、この脆弱性（CVE-2016-5195）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 2.6.22 および、それ以降の以下のバージョンが影響を受けます。

- Linux Kernel 4.8.3 より前のバージョン
- Linux Kernel 4.7.9 より前のバージョン
- Linux Kernel 4.4.26 より前のバージョン

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

（実行例）

```
pentest@debian77:/$ uname -r
3.2.0-4-amd64
pentest@debian77:/$
```

【対策案】

この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ます。

また、各ベンダーからリリースされている当該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、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、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。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】

- CVE-2016-5195
- JVNVU#91983575 Linux カーネルのメモリサブシステムに実装されている copy-on-write 機構に競合状態が発生する脆弱性
- Vulnerability Note VU#243144 – Linux kernel memory subsystem copy on write mechanism contains a race condition vulnerability

Linux Kernel

- ChangeLog-4.8.3
- ChangeLog-4.7.9
- ChangeLog-4.4.26

Linux ディストリビューション

- CVE-2016-5195 (Debian)
- CVE-2016-5195 in Ubuntu
- CVE-2016-5195 - Red Hat Customer Portal
- CVE-2016-5195 | SUSE
- ALAS-2016-757 (Amazon Linux)

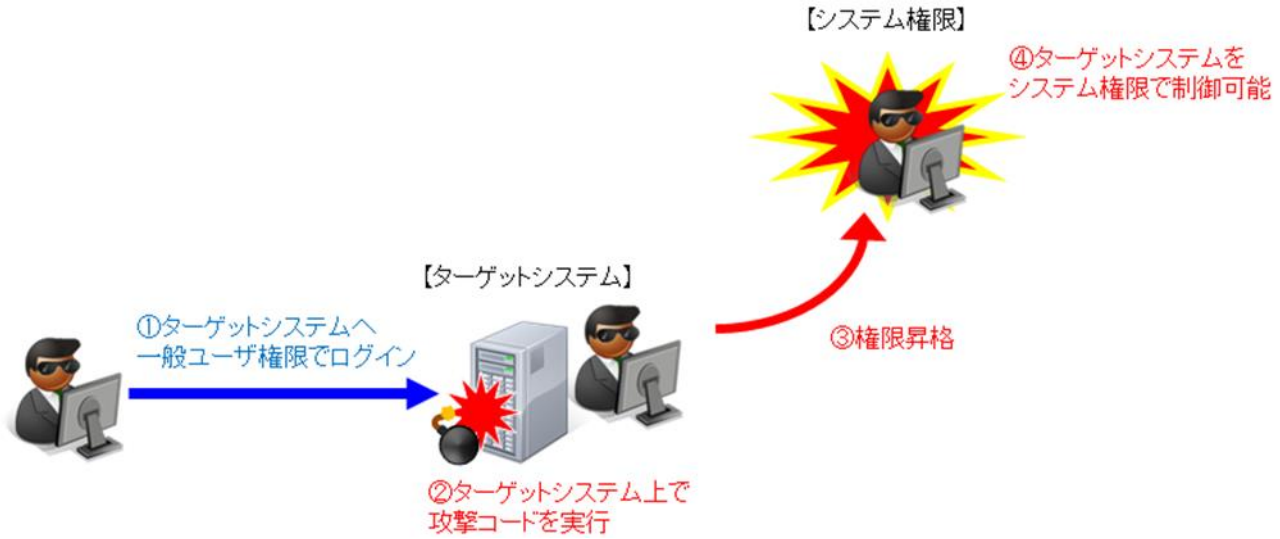
【検証概要】

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、管理者権限(root)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】

Debian 7.8 + Kernel 3.2.0-4-amd64

【検証イメージ】



【検証結果】

下図は、ターゲットシステム（Debian）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ました。

```
pentest@debian77: ~/CVE-2016-5195
ファイル(F)  編集(E)  表示(V)  検索(S)  端末(T)  ヘルプ(H)
pentest@debian77:~/CVE-2016-5195$ uname -an
Linux debian77 3.2.0-4-amd64 #1 SMP Debian 3.2.65-1+deb7u2 x86_64 GNU/Linux
pentest@debian77:~/CVE-2016-5195$ uname -r
3.2.0-4-amd64
pentest@debian77:~/CVE-2016-5195$ whoami
pentest
pentest@debian77:~/CVE-2016-5195$ id
uid=1000(pentest) gid=1000(pentest) groups=1000(pentest),24(cdrom),25(floppy),29(a
udio),30(dip),44(video),46(plugdev),104(scanner),107(bluetooth),109(netdev)
pentest@debian77:~/CVE-2016-5195$ ./cowroot
DirtyCow root privilege escalation
Backing up /usr/bin/passwd.. to /tmp/bak
Size of binary: 51096
Racing, this may take a while..
/usr/bin/passwd is overwritten
Popping root shell.
Don't forget to restore /tmp/bak
thread stopped
thread stopped
root@debian77:/home/pentest/CVE-2016-5195# whoami
root
root@debian77:/home/pentest/CVE-2016-5195# id
uid=0(root) gid=1000(pentest) groups=0(root),24(cdrom),25(floppy),29(audio),30(dip
),44(video),46(plugdev),104(scanner),107(bluetooth),109(netdev),1000(pentest)
root@debian77:/home/pentest/CVE-2016-5195#
```

【更新履歴】

2016 年 10 月 25 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/