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

GNU C ライブラリ(glibc)のリモートから任意のコードを実行可能な脆弱性(CVE-2015-7547)に関する調査レポート

【概要】

Linux 等で広く用いられている、GNU C ライブラリ(以下、glibc と記載)に、リモートより任意のコードが実行可能であると報告された脆弱性(CVE-2015-7547)の実証コード(PoC(*1))が発見されました。

この脆弱性は glibc 内の getaddrinfo()関数において、細工された DNS クエリを特定の条件化において適切に処理できないためにおこります。結果、リモートから任意のコードを実行される可能性があります。これにより、攻撃者があらかじめ用意した DNS サーバーに、攻撃対象システムからの名前解決を実行させることにより、この脆弱性を利用するといった攻撃が可能となります。また、信頼できる DNS サーバーを利用している場合でも通信経路が信頼できない場合、中間者攻撃により経路上で通信が改ざんされてしまい本脆弱性の影響を受ける可能性があります。

本レポート作成(2 月 22 日)時点において、 glibc project よりこの脆弱性が修正するパッチ、各ベンダーからアップデートプログラムがリリースされております。また、現時点(2 月 22 日)において、該当する脆弱性を利用する攻撃コードの公開は確認されておりませんが、影響が大きいと判断されるため、今回は公開された実証コードを用いて検証を行いました。

**1 PoC(Proof-of-Concept の略):脆弱性の概念(コンセプト)を実証するための検証プログラム、脆弱性の存在を証明するために用いられる。*

【影響を受ける可能性があるシステム】

- glibc 2.9 から 2.22 までを使用するシステム
  - Red Hat
    - Red Hat Enterprise Linux Server EUS (v. 6.6)
    - Red Hat Enterprise Linux Server AUS (v. 6.5)
    - Red Hat Enterprise Linux Server AUS (v. 6.4)
    - Red Hat Enterprise Linux Server AUS (v. 6.2)
    - Red Hat Enterprise Linux Server EUS (v. 7.1)
    - Red Hat Enterprise Linux version 6
    - Red Hat Enterprise Linux version 7
  - Debian
    - Debian 6.0(squeeze)
    - Debian 7.0(wheezy)
    - Debian 8.0(jessie)
  - Ubuntu
    - Ubuntu 15.10

- Ubuntu 14.04 LTS
- Ubuntu 12.04 LTS

- Asianux Server
  - Asianux Server 4 == MIRACLE LINUX V6 for x86 (32bit)
  - Asianux Server 4 == MIRACLE LINUX V6 for x86_64 (64bit)
  - Asianux Server 7 == MIRACLE LINUX V7 for x86_64 (64bit)

【対策案】

glibc project より脆弱性に対する対策パッチ、また各ベンダーより、この脆弱性を修正するパッケージがリリースされています。当該脆弱性が修正されたバージョンへとアップグレードしていただくことを推奨いたします。また、アップグレード後 glibc を利用しているサービスの再起動を実施してください。

（影響緩和策）

利用する DNS サーバーについて、ユーザーが信頼できる自組織のもののみを利用することにより、悪意を持つ DNS 応答を直接受け取る可能性を低減します。また、DNS リゾルバが受け入れるレスポンスサイズを、TCP,UDP 共に 2048 バイトを超えないように制限します。ただし権威 DNSサーバーとフルリゾルバ(*2)の間の通信は当該脆弱性の対象外なので制限の必要はありません。

参考：（緊急）GNU C Library（glibc）の脆弱性について（CVE-2015-7547）

https://jprs.jp/tech/security/2016-02-18-glibc-vuln-getaddrinfo.html

**2 フルサービスリゾルバ:問い合わせに対し、自らもしくは、他の DNS サーバーに名前解決の問い合わせをし、問い合わせ元に結果を返す DNS サーバー、フルリゾルバ、キャッシュ DNS サーバーとも言う。*

【glibc のバージョンの確認方法(RedHat/CentOS の場合)】

ターミナル上で以下のコマンドを実行することにより、インストールされている glibc のバージョンを確認することが可能です。

```
$ yum -q list installed glibc
```

【glibc のバージョンの確認方法(Debian)の場合)】

```
$ dpkg -l libc6
```

(Debianの場合は libc6 パッケージに glibc が含まれています)

参考(Debian 7.0(wheezy)の場合)：https://packages.debian.org/wheezy/libc6

【glibc を利用しているプロセスの確認方法】

```
$ lsof | grep 'libc-'
```

【参考サイト】

- CVE-2015-7547
- JVNDB-2016-001419 - JVN iPedia - 脆弱性対策情報データベース
- JVNVU#97236594: glibc にバッファオーバーフローの脆弱性
- <<< JPCERT/CC Alert 2016-02-17 >>> glibc ライブラリの脆弱性（CVE-2015-7547）に関する注意喚起
- CVE-2015-7547 - Red Hat Customer Portal
- glibc の脆弱性(CVE-2015-7547)の影響と対処 ― MIRACLE LINUX CORPORATION

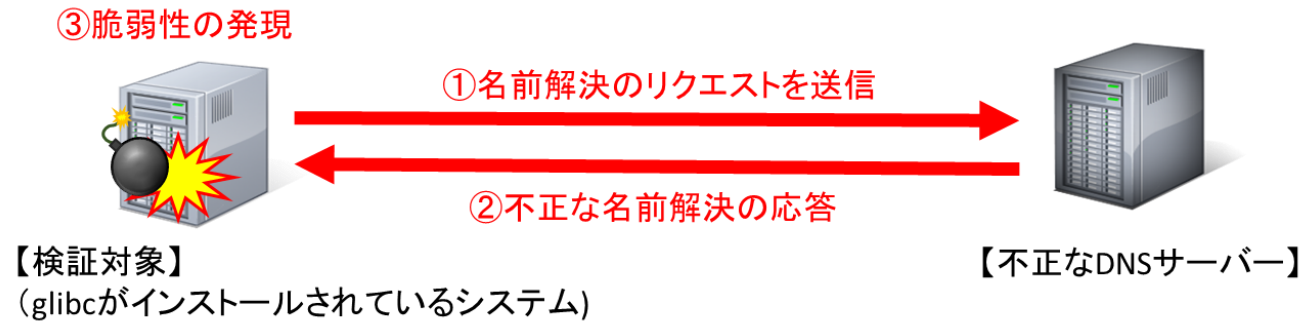
【検証概要】

今回は、脆弱性の存在の有無を確認する実証コードを実行し、該当システム（Debian・CentOS）に脆弱性があるかの確認をしました。

【検証ターゲットシステム】

OS	パッケージ名	バージョン
Debian7.7	libc6	2.13-38+deb7u8
CentOS7	glibc.x86_64	2.17-55.el7

【検証イメージ】



【検証結果】

下図は、不正な DNS サーバー(10.0.0.103)として稼動しているホストです。黄線の部分は、実証コードを実行している箇所です。

```
[root@testOS CVE-2015-7547-master]# ifconfig ens160
ens160: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 10.0.0.103  netmask 255.255.255.0  broadcast 10.0.0.255
        inet6 fe80::20c:29ff:fec2:deef  prefixlen 64  scopeid 0x20<link>
        ether 00:0c:29:c2:de:ef  txqueuelen 1000  (Ethernet)
        RX packets 3140  bytes 321735 (314.1 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 1200  bytes 310739 (303.4 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

[root@testOS CVE-2015-7547-master]# python CVE-2015-7547-poc.py
[UDP] Total Data len recv 36
[UDP] Total Data len recv 36
Connected with 10.0.0.177:35290
[TCP] Total Data len recv 76
[TCP] Request1 len recv 36
[TCP] Request2 len recv 36
```

下図は、検証対象(Debian)の画面です。赤線で囲まれている部分が、実行結果の応答情報です。名前解決のリクエストを、不正な DNS サーバーに送信し応答を受けることにより、脆弱性が発現します。これにより、検証対象で該当する脆弱性が存在することが確認できました。

*CentOS7 においても、同じ検証結果を確認済みです。

```
root@debian77:~# uname -an
Linux debian77 3.2.0-4-amd64 #1 SMP Debian 3.2.65-1+deb7u2 x86_64 GNU/Linux
root@debian77:~# dpkg -l libc6
要望=(U)不明/(I)インストール/(R)削除/(P)完全削除/(H)保持
| 状態=(N)無/(I)インストール済/(C)設定/(U)展開/(F)設定失敗/(H)半インストール/(W)トリガ待ち/(T)トリガ保留
|/ エラー?=(空欄)無/(R)要再インストール (状態,エラーの大文字=異常)
||/ 名前           バージョ アーキテ 説明
+++-==============-============-============-================================
ii  libc6:amd64    2.13-38+deb7 amd64        Embedded GNU C Library: Shared lib
root@debian77:~# nslookup
> server
Default server: 10.0.0.103
Address: 10.0.0.103#53
> exit

root@debian77:~# ssh softbanktech.co.jp
Segmentation fault
root@debian77:~#
```

【更新履歴】

2016 年 2 月 25 日 ： 影響を受ける可能性があるシステムに AsianuxServer を追加、参考サイトにミラクル・リナックス株式会社セキュリティアップデート情報を追加

2016 年 2 月 22 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/