

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

### BIND の TKEY リソースレコードの処理に起因するリモートからサービス拒否攻撃を実行可能な脆弱性 (CVE-2015-5477)に関する調査レポート

#### 【概要】

Internet Systems Consortium (以下、ISC)の BIND に、リモートよりサービス拒否攻撃が可能な脆弱性(CVE-2015-5477)の攻撃コードが発見されました。この脆弱性は、TKEY リソースレコード(RR)の処理に欠陥があり、TKEY RR に対して細工された問い合わせを行うことによりサービス拒否状態を引き起こすことが可能です。

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 BIND を停止させることが可能です。

本レポート作成(2015年8月5日)時点において、既にISCより脆弱性が修正されたバージョンがリリースされています(2015年7月28日)。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-2015-5477)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】

- BIND 9.1.0 から 9.8.x までの全てのバージョン
- BIND 9.9.0 から 9.9.7-P1 までの全てのバージョン
- BIND 9.10.0 から 9.10.2-P2 までの全てのバージョン

#### 【対策案】

本レポート作成(2015年8月5日)時点において、ISCより、この脆弱性を修正するバージョン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。

なお、BIND 9.8.x よりも前のバージョンはサポートが終了しています。該当するバージョンを利用されている場合、本脆弱性を修正するためには、バージョン 9.9.7-P2、または、9.10.2-P3 へとアップグレードしていただく必要があります。

#### 【参考サイト】

- [CVE-2015-5477](#)
- [DNS サーバ BIND の脆弱性対策について\(CVE-2015-5477\)](#)
- [ISC BIND 9 サービス運用妨害の脆弱性 \(CVE-2015-5477\) に関する注意喚起](#)

#### 【検証概要】

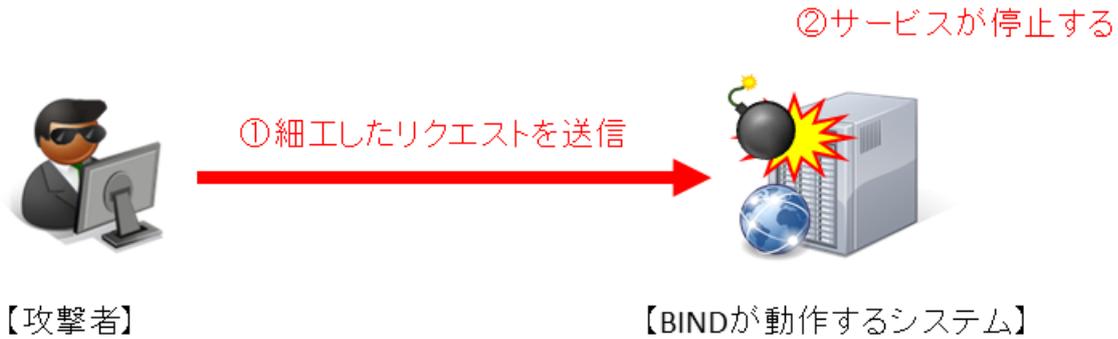
ターゲットシステムに対して、攻撃者が細工したクエリを送信することにより、ターゲットシステム上で動作している

BIND を停止させます。

【検証ターゲットシステム】

Debian 8 + BIND 9.9.7-P1

【検証イメージ】



【検証結果】

下図の、上段のターミナル画面は攻撃側の画面です。一方で、下段のターミナル画面はターゲットシステム(Linux)の画面です。黄線で囲まれた部分は、攻撃者により細工されたクエリを送信される前の、動作している BIND の情報です。BIND がオープンするポート番号(TCP/53, UDP/53)が開放されていることが確認できます。

一方で、赤線で囲まれている部分は、攻撃者により細工されたクエリを送信された後の BIND の情報です。BIND がオープンするポート番号(TCP/53, UDP/53)が一覧から消えたことが確認できます。

これにより、ターゲットシステムの BIND が停止したと判断できます。

```

172.20.10.9:22 - pentest@Penux: ~/exploit VT
ファイル(F) 編集(E) 設定(S) コントロール(O) ウィンドウ(W) ヘルプ(H)
pentest@Penux:~/exploit$ /sbin/ifconfig eth0
eth0      Link encap:イーサネット  ハードウェアアドレス 00:0c:29:6c:a7:ae
          inetアドレス:172.20.10.9  ブロードキャスト:172.20.10.15  マスク:255.255.255.240
          inet6アドレス: fe80::20c:29ff:fe6c:a7ae/64  範囲:リンク
          UP BROADCAST RUNNING MULTICAST  MTU:1500  メトリック:1
          RXパケット:423 エラー:0 損失:0  オーバラン:0  フレーム:0
          TXパケット:300 エラー:0 損失:0  オーバラン:0  キャリア:0
          衝突(Collision):0 TXキュー長:1000
          RXバイト:46926 (45.8 KiB) TXバイト:45285 (44.2 KiB)

pentest@Penux:~/exploit$ ./cve20155477 172.20.10.11
--- PoC for CVE-2015-5477 BIND9 TKEY assert DoS ---
[+] 172.20.10.11: Resolving to IP address
[+] 172.20.10.11: Resolved to multiple IPs (NOTE)
[+] 172.20.10.11: Probing...
[+] Querying version...
[+] 172.20.10.11: "NameServer"
[+] Sending DoS packet...
[+] Waiting 5-sec for response...
[+] timed out, probably crashed

pentest@Penux:~/exploit$ █

172.20.10.11:22 - testuser@nsbian: ~ VT
ファイル(F) 編集(E) 設定(S) コントロール(O) ウィンドウ(W) ヘルプ(H)
root@nsbian:~# ifconfig eth0
eth0      Link encap:イーサネット  ハードウェアアドレス 00:0c:29:63:a4:02
          inetアドレス:172.20.10.11  ブロードキャスト:172.20.10.15  マスク:255.255.255.240
          inet6アドレス: fe80::20c:29ff:fe63:a402/64  範囲:リンク
          UP BROADCAST RUNNING MULTICAST  MTU:1500  メトリック:1
          RXパケット:447 エラー:0 損失:0  オーバラン:0  フレーム:0
          TXパケット:318 エラー:0 損失:0  オーバラン:0  キャリア:0
          衝突(Collision):0 TXキュー長:1000
          RXバイト:50190 (49.0 KiB) TXバイト:45130 (44.0 KiB)

root@nsbian:~# date
2015年  8月  4日  火曜日 18:16:48 JST
root@nsbian:~# lsof -i -n -P -R |grep named
named    737    1      bind    20u    IPv4    12598      0t0  TCP    127.0.0.1:53 (LISTEN)
named    737    1      bind    21u    IPv4    12600      0t0  TCP    172.20.10.11:53 (LISTEN)
named    737    1      bind    22u    IPv4    12601      0t0  TCP    127.0.0.1:953 (LISTEN)
named    737    1      bind    512u   IPv4    12597      0t0  UDP    127.0.0.1:53
named    737    1      bind    513u   IPv4    12599      0t0  UDP    172.20.10.11:53

root@nsbian:~# █
root@nsbian:~# date
2015年  8月  4日  火曜日 18:17:05 JST
root@nsbian:~# lsof -i -n -P -R |grep named
root@nsbian:~# █

```

この脆弱性による攻撃を受けた場合、BIND のログに以下のような情報が記述されます。

※以下はソース版の BIND を Debian ヘインストールした場合の例です。ログのパスは /var/named/chroot/var/log を設定しています。Linux のパッケージを利用されている場合や、OS または BIND の構成環境によって出力されるログのパスや内容は異なります。

/var/named/chroot/var/log/named.log の内容

```

root@nsbian:/var/named/chroot/var/log# cat named.log
04-Aug-2015 01:31:47.881 general: managed-keys-zone: loaded serial 0
04-Aug-2015 01:31:47.882 general: zone 10.20.172.in-addr.arpa/IN: loaded serial 2015080409
04-Aug-2015 01:31:47.882 general: zone test.local/IN: loaded serial 2015080409
04-Aug-2015 01:31:47.883 general: all zones loaded
04-Aug-2015 01:31:47.883 general: running
04-Aug-2015 01:32:34.318 general: message.c:2328: REQUIRE(*name == ((void *)0)) failed
04-Aug-2015 01:32:34.318 general: exiting (due to assertion failure)
04-Aug-2015 01:33:18.259 general: managed-keys-zone: loaded serial 0
04-Aug-2015 01:33:18.260 general: zone 10.20.172.in-addr.arpa/IN: loaded serial 2015080409
04-Aug-2015 01:33:18.260 general: zone test.local/IN: loaded serial 2015080409
04-Aug-2015 01:33:18.260 general: all zones loaded
04-Aug-2015 01:33:18.261 general: running
04-Aug-2015 01:33:33.857 general: message.c:2328: REQUIRE(*name == ((void *)0)) failed
04-Aug-2015 01:33:33.857 general: exiting (due to assertion failure)
04-Aug-2015 01:33:59.809 general: managed-keys-zone: loaded serial 0
04-Aug-2015 01:33:59.810 general: zone 10.20.172.in-addr.arpa/IN: loaded serial 2015080409
04-Aug-2015 01:33:59.810 general: zone test.local/IN: loaded serial 2015080409
04-Aug-2015 01:33:59.810 general: all zones loaded
04-Aug-2015 01:33:59.810 general: running
04-Aug-2015 01:34:11.507 general: message.c:2328: REQUIRE(*name == ((void *)0)) failed
04-Aug-2015 01:34:11.507 general: exiting (due to assertion failure)
root@nsbian:/var/named/chroot/var/log#

```

『message: REQUIRE failed (assertion failure)』が記述されます。

#### 【更新履歴】

2015年8月5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/>