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

BIND の脆弱性により、リモートからサービス拒否攻撃を実行可能な脆弱性（CVE-2016-2776）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-2016-2776）の攻撃コードが発見されました。この脆弱性は、細工された DNS クエリを受信した際に buffer.c でアサーションエラーが起きることに起因し、結果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（2016 年 10 月 6 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おります（2016 年 9 月 27 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、また既にこの脆弱性を利用した攻撃により、実際に DNS サービスが停止した被害報告が出ていることから、今回この脆弱性（CVE-2016-2776）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 9.0.x から 9.8.x までの全てのバージョン
- BIND 9.9.0 から 9.9.9-P2 までの全てのバージョン
- BIND 9.9.3-S1 から 9.9.9-S3 までの全てのバージョン
- BIND 9.10.0 から 9.10.4-P2 までの全てのバージョン
- BIND 9.11.0a1 から 9.11.0rc1 までの全てのバージョン

【対策案】

本レポート作成（2016 年 10 月 6 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 9.9.9-P3、または、9.10.4-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-2016-2776
- DNS サーバ BIND の脆弱性対策について(CVE-2016-2776)
- ISC BIND 9 サービス運用妨害の脆弱性（CVE-2016-2776）に関する注意喚起

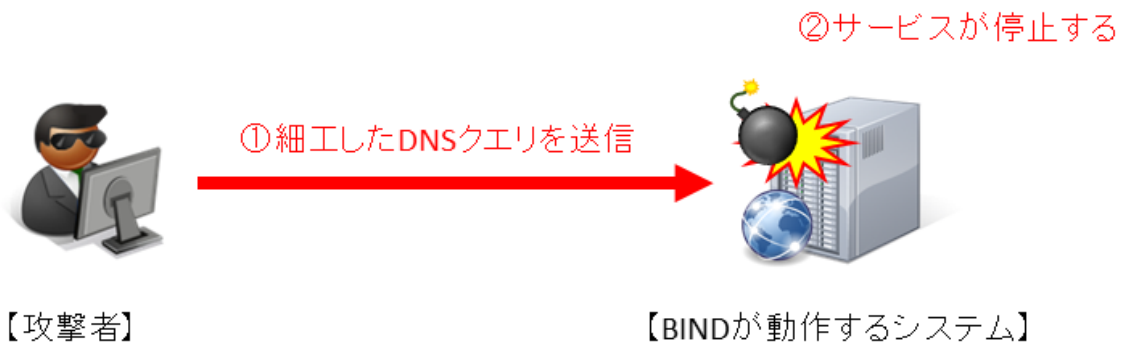
【検証概要】

ターゲットシステムに対して、攻撃者が細工した DNS 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】

Ubuntu 16.04 + BIND 9.9.9-P2

【検証イメージ】

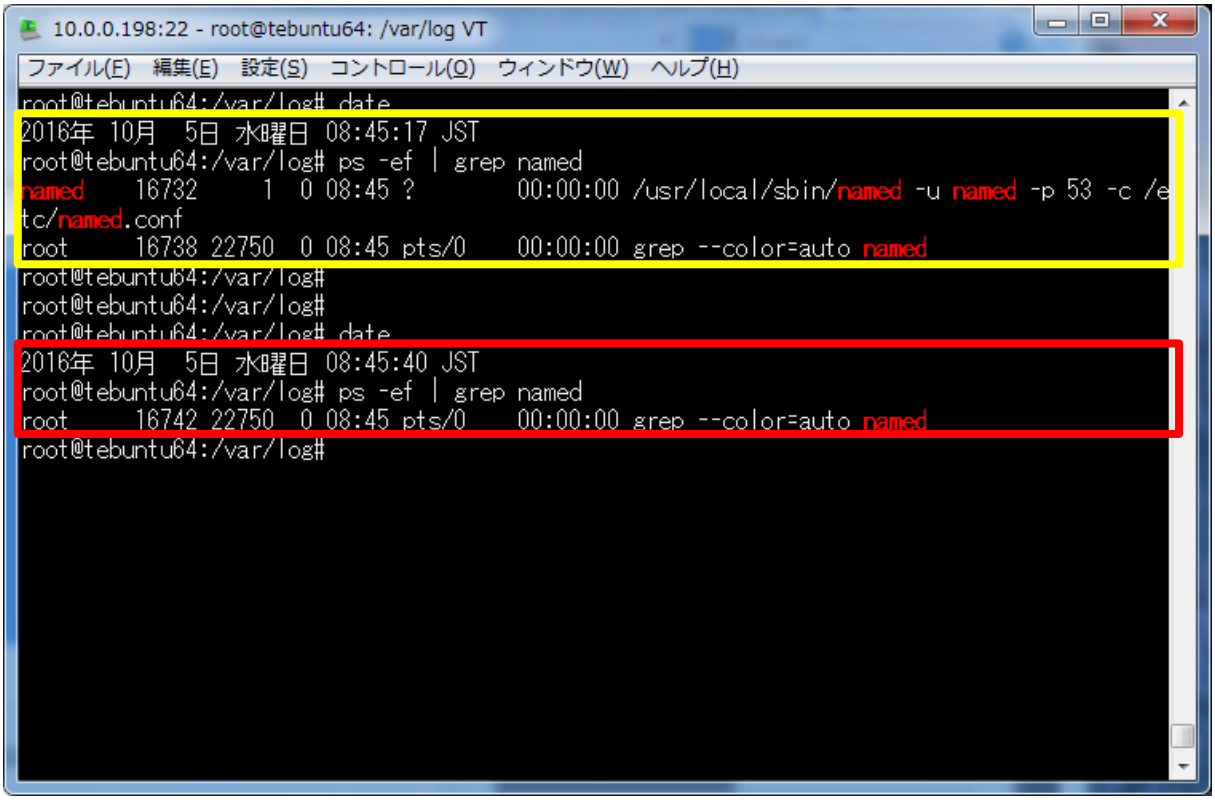


【検証結果】

下図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 DNS クエリを送信される前の動作している BIND の情報です。プロセス一覧に BIND（プロセス名 named）が動作し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 DNS クエリを送信された後の BIND の情報です。プロセス一覧から BIND のプロセスである named が消えたことが確認できます。

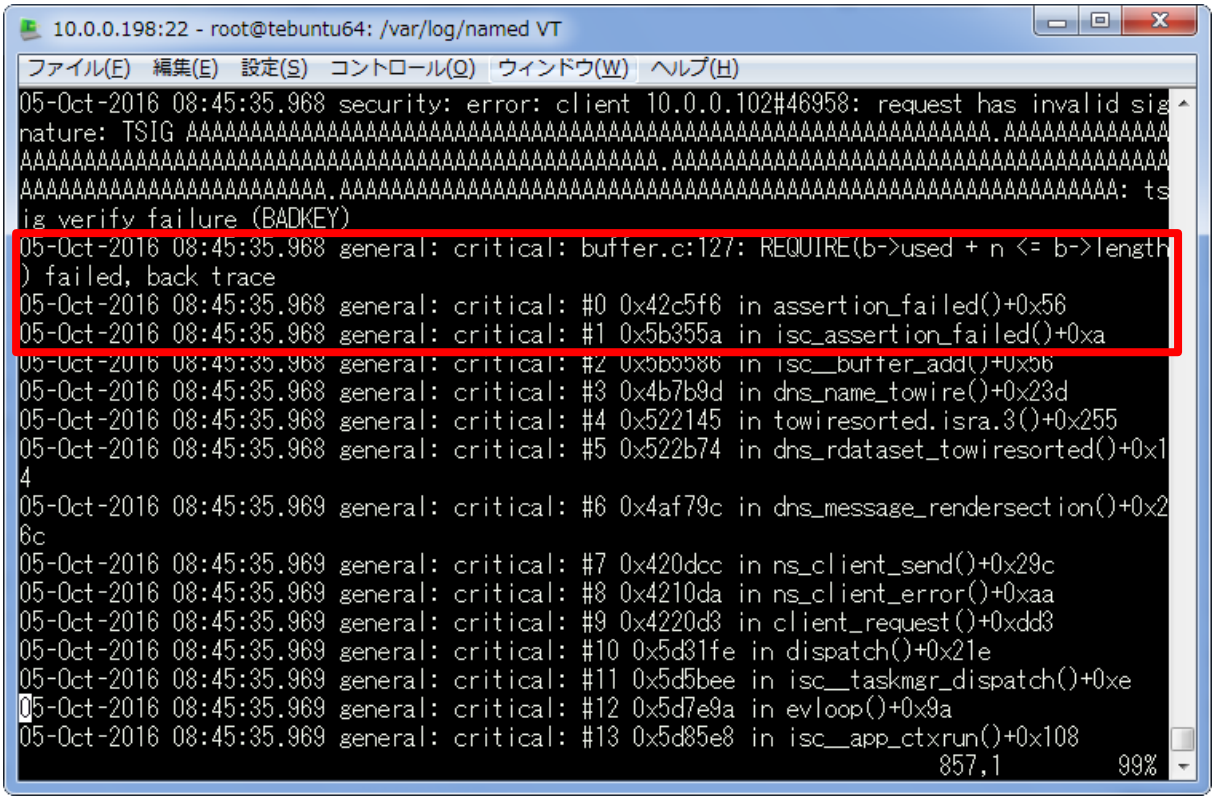
これにより、ターゲットシステムの BIND が停止したと判断できます。



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

※以下はソース版の BIND を Ubuntu へインストールした場合の例です。ログのパスは /var/log/named 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/log/named/default.log の内容



buffer.c における assertion failure が記述されます。

【更新履歴】

2016 年 10 月 6 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/