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

NTP 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-2016-7434）に関する調査レポート

【概要】

NTP Project の NTP に、リモートよりサービス拒否攻撃が可能な脆弱性（CVE-2016-7434）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 mrulist クエリを受信した際の入力値チェックに不備があり、ntpd がクラッシュします。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 NTP を停止させることが可能です。

本レポート作成（2016 年 11 月 28 日）時点において、既に NTP Project 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 11 月 21 日）。しかしながら、攻撃を成立させるためのコードの入手可能および、攻撃が容易であることから、今回この脆弱性（CVE-2016-7434）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】

- NTP 4.2.7p22 から 4.2.8p8 までの全てのバージョン
- NTP 4.3.0 から 4.3.93 までの全てのバージョン

【対策案】

本レポート作成（2016 年 11 月 28 日）時点において、NTP Project 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。

【参考サイト】

- CVE-2016-7434
- JVNVU#99531229 NTP.org の ntpd に複数の脆弱性
- November 2016 ntp-4.2.8p9 NTP Security Vulnerability Announcement (HIGH for Windows, MEDUIM otherwise)

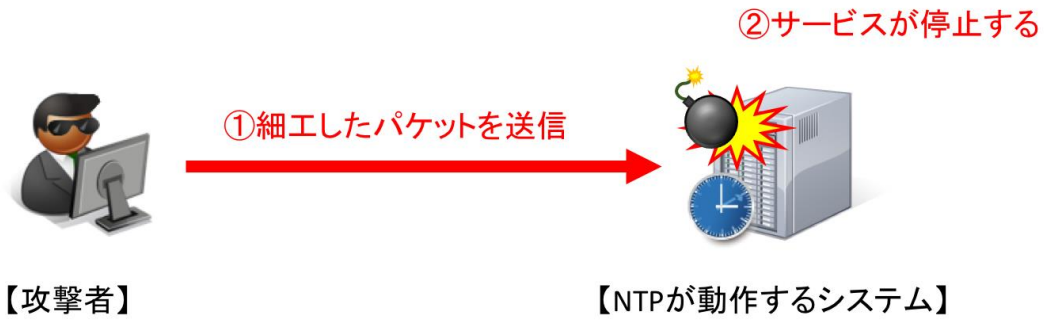
【検証概要】

ターゲットシステムに対して、攻撃者が細工したパケット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 NTP サービスを停止させます。

【検証ターゲットシステム】

Debian 8.6 + NTP 4.2.8p8

【検証イメージ】

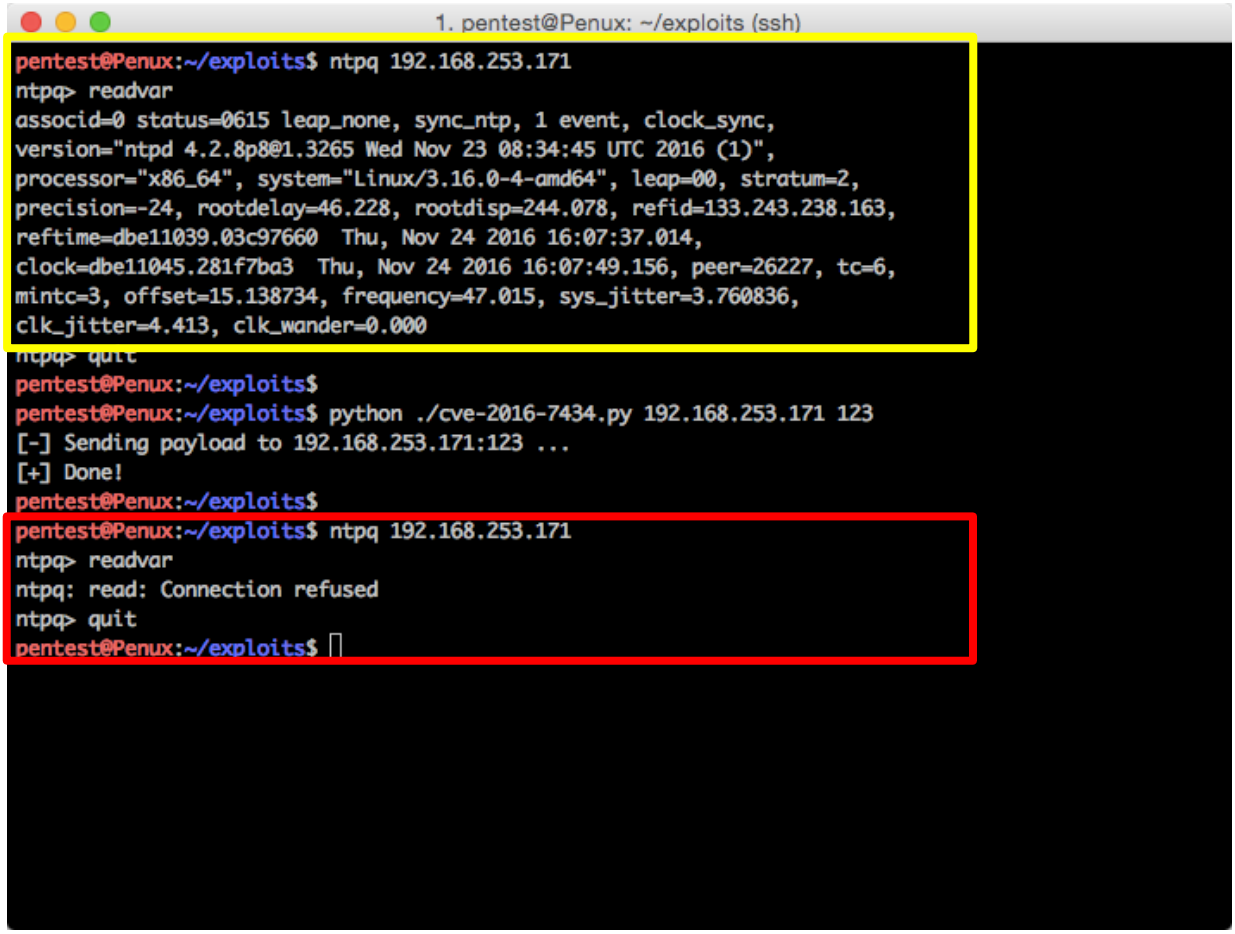


【検証結果】

下図のターミナル画面は攻撃者側のシステム（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パケットを送信される前の、動作している NTP サービスへ問い合わせを行った結果です。

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パケットを送信された後に NTP サービスへ問い合わせを行った結果です。細工されたパケットを送信する前後で、NTP サービスの応答が無くなったこと（Connection Refused）が確認できます。

（攻撃側の画面）

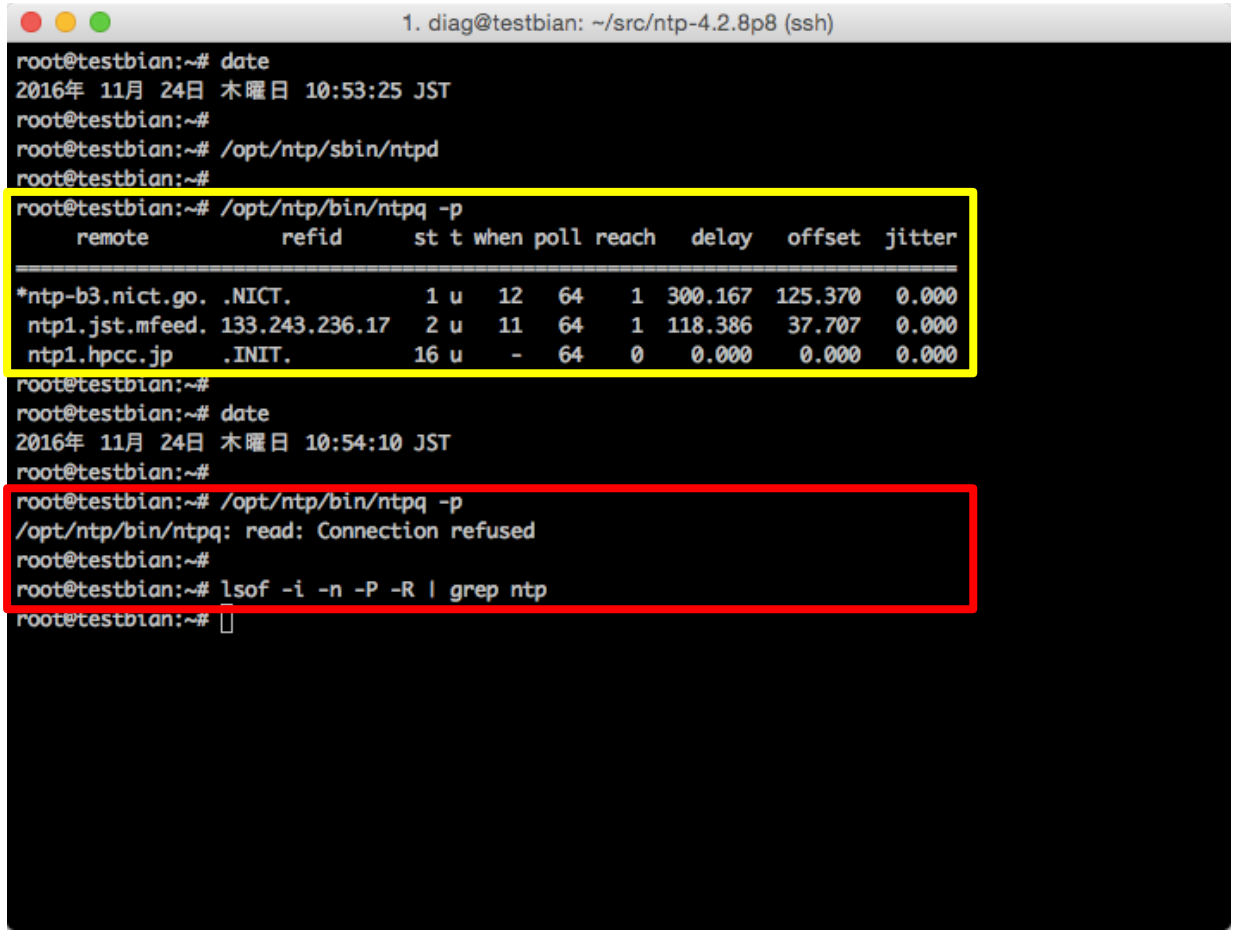


下図のターミナル画面はターゲットシステム（Linux）の画面です。黄線で囲まれた部分は、攻撃者により細工されたパケットを送信される前の動作している NTP サービスの情報です。NTP サービスにおいて、ピアリストが表示されている（ntpq –p コマンドの出力結果）ことが確認できます。

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パケットを送信された後の NTP サービスの情報です。ピアリストを表示するコマンドを送信しても応答が無く、また NTP サービスが利用しているポート（UDP/123）が閉じていること（lsof –i –n –P –R コマンドの出力結果）が確認できます。

これにより、ターゲットシステムの NTP サービスが停止したと判断できます。

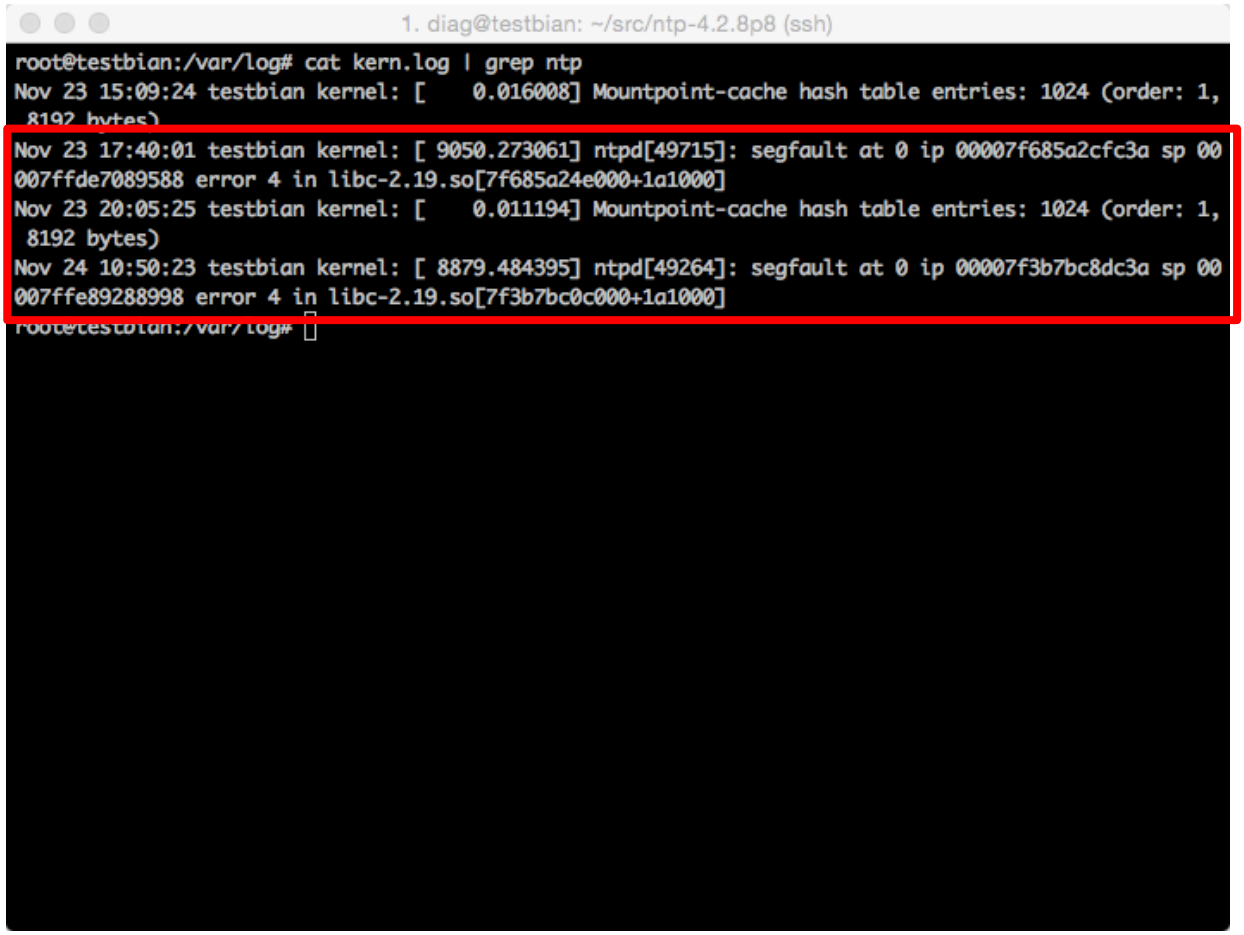
（被攻撃側の画面）



この脆弱性による攻撃を受けた場合、カーネル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 NTP を Debian へインストールした場合の例です。ログのパスは /var/log/kern.log です。Linux のパッケージを利用されている場合や、OS または NTP 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/kern.log の内容



ntpd における セグメンテーション違反（segfault）が記述されます。

【更新履歴】

2016 年 11 月 28 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/