株式会社 日立システムズ

SSRC-VR-20140411
発行日:2013/04/11

S.S.R.C.

脆弱性検証レポート

(CVE-2014-0160)

株式会社　日立システムズ

セキュリティリサーチセンタ

S.S.R.C.脆弱性検証レポート

目次

1. はじめに

S.S.R.C.(Shield Security Research Center)は、株式会社日立システムズ　セキュリティリサーチセンタが運営するセキュリティ情報公開サイトです。本サイトでは、セキュリティリサーチセンタによるリサーチ結果を随時配信する予定です。

本文書は、株式会社日立システムズ、SHIELD セキュリティセンタで日々収集を行っている世界中のセキュリティトレンド情報にもとづき、セキュリティリサーチセンタのセキュリティアナリストが確認した、ソフトウェア等の脆弱性検証結果をまとめたレポートです。

次に示す、ご利用条件を十分にお読み頂き、ご了承頂いた上でご利用頂きます様、よろしくお願い致します。

2. ご利用条件

本文書内の文章等すべての情報掲載に当たりまして、株式会社日立システムズ（以下、「当社」といいます。）と致しましても細心の注意を払っておりますが、その内容に誤りや欠陥があった場合にも、いかなる保証もするものではありません。本文書をご利用いただいたことにより生じた損害につきましても、当社は一切責任を負いかねます。

本文書に掲載されている情報は、掲載した時点での情報です。掲載した時点以降に変更される場合もありますので、あらかじめご了承ください。

3. 概要

3.1. 脆弱性の概要

2014 年 4 月 7 日(米国時間)、OpenSSL の HeartBeat 機能の実装に関する脆弱性(CVE-2014-0160)が発表されました。

この脆弱性を悪用されると、システム上のメモリデータが窃取される可能性があります。例えば、SSL 証明書に関する秘密鍵が窃取されている可能性があります。

3.2. 影響を受けるシステム

以下の OpenSSL のバージョンに影響があります。

- OpenSSL 1.0.1 から 1.0.1f まで
- OpenSSL 1.0.2-beta から 1.0.2-beta1 まで

また、上記バージョンの OpenSSL を利用しているウェブサーバやメールサーバなどのプログラムも影響を受けます。

3.3. 影響の有無の確認方法

以下のいずれかの方法で確認してください。

1. openssl コマンドを利用したバージョンと HeartBeat 機能の有効化状況の確認

```
$ openssl version -a
```

2. オンラインスキャナーで確認

http://filippo.io/Heartbleed/

https://sslcheck.globalsign.com/ja

http://ssl.white.hacker.jp/hb/hb

https://www.ssllabs.com/ssltest/index.html

http://possible.lv/tools/hb/

3.4. 深刻度

深刻度:注意

CVSS 基本値:5.0 [SSRC 評価]

3.5. 対策方法

- 根本対策

  本脆弱性が修正されたバージョンにアップデートしてください。

- 回避策

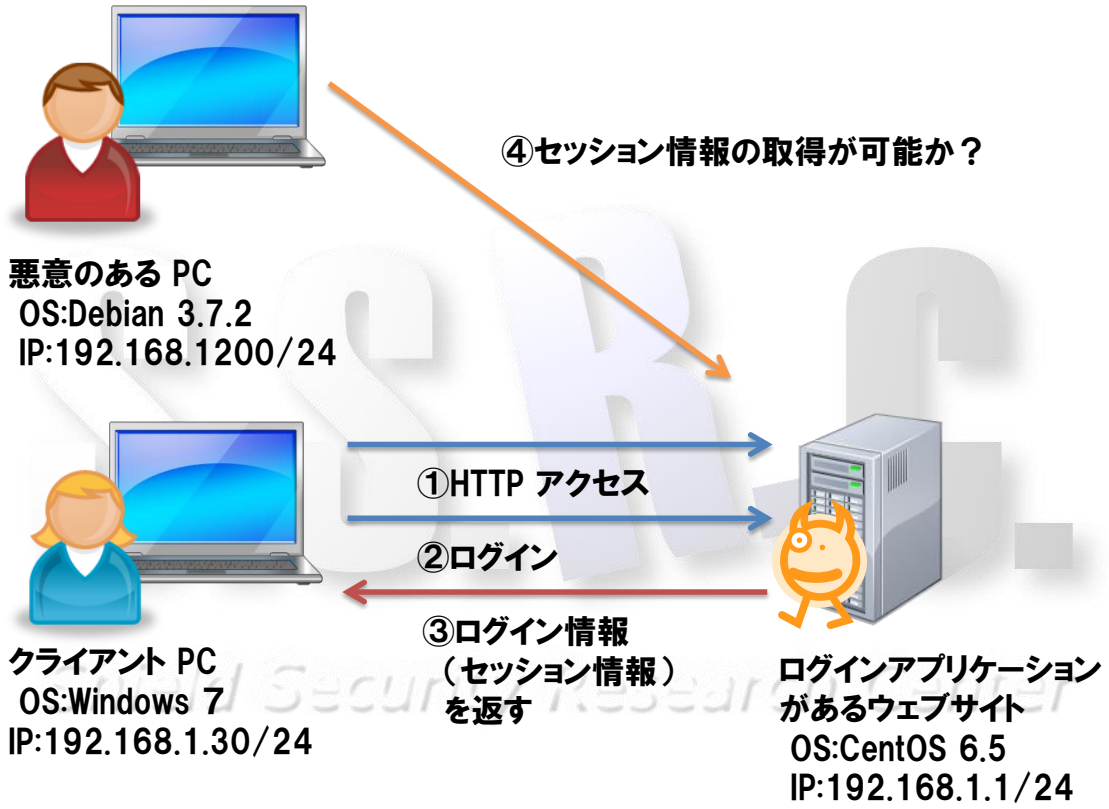
  「-DOPENSSL_NO_HEARTBEATS」フラグを指定して再コンパイルし、HeartBeat 機能を無効にしてください。

- 追加対策

  既に本脆弱性を悪用した攻撃を受けて、SSL サーバ証明書の秘密鍵や認証情報などが漏洩している可能性があります。根本的対策を実施した上で、必要に応じて、サーバ証明書の更新や認証情報の変更などを実施してください。

4. 検証

本検証のイメージは下記のとおりです。クライアント PC(Windows 7)から、ログイン機能をもつウェブサーバ(CentOS)にアクセスし、ログイン機能を持つウェブアプリケーションにログインします。次に、悪意のある PC から(Ubuntu)からウェブサーバに接続し、クライアント PC のログイン情報(セッション情報)を取得が可能かを検証します。本検証では、一般に公開されているいくつかの情報源から集めた検証コードをもとに検証を実施しました。



4.1. 脆弱なバージョンの OpenSSL を利用した検証

- **検証環境**

ウェブサーバ：

OS　　：CentOS 6.5

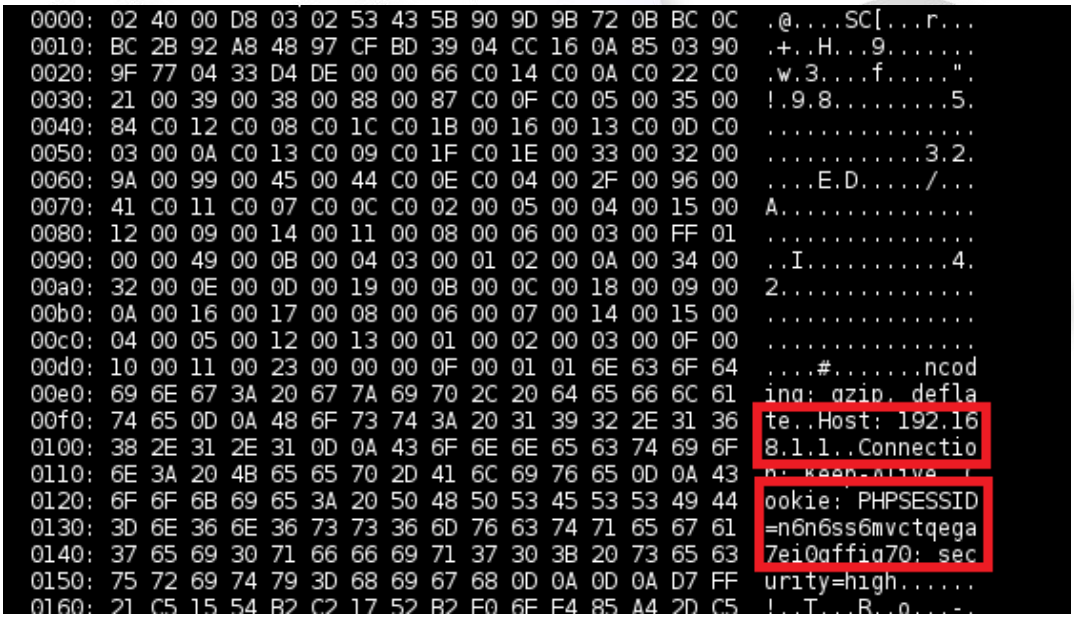
Apache　：Apache 2.2.15

PHP　　：PHP 5.3.3

OpenSSL　：OpenSSL 1.0.1e-15.el6

- **検証結果**

下図は、悪意のある PC のターミナル画面です。本脆弱性を悪用され、ログイン情報（セッション情報）が取得出来ていることがわかります。



4.2. 修正済みバージョンの OpenSSL を利用した検証

- **検証環境**

ウェブサーバ：

OS　　：CentOS 6.5
Apache　：Apache 2.2.15
PHP　　：PHP 5.3.3
OpenSSL　：OpenSSL 1.0.1e-16.7

※ RHEL 系のパッケージソフトウェアのバージョンは、オリジナルのバージョンとは異なる場合があります。
本バージョンで修正されていることは下記のコマンドで確認しております。

```
# rpm -q --changelog openssl | more

* 月  4 月 07 2014 Tomáš Mráz <tmraz@redhat.com> 1.0.1e-16.7

- fix CVE-2014-0160 - information disclosure in TLS heartbeat extension
```

- **検証結果**

「4.1 脆弱なバージョンの OpenSSL を利用した検証」と同様の手順で検証を実施しましたが、ウェブサーバから、ログイン情報（セッション情報）の取得は出来ませんでした。

5. まとめ

影響を受けるバージョンの OpenSSL を利用した検証では、現時点で公開されている検証コードを用いることで、ログイン情報の窃取が可能でしたが、本脆弱性の**修正済みバージョンの OpenSSL を利用した検証では、ログイン情報の窃取が出来ないことを確認**しました。結果、最新版の OpenSSL で、本脆弱性は修正されていると判断できます。

しかし、**すでに情報が窃取されてしまっている可能性がありますので、アップデートの実施と共に、追加対策(3.5 対策方法を参照)の実施を推奨**します。

[参考文献]

- ベンダ情報

（i）. https://www.openssl.org/news/secadv_20140407.txt

- その他情報

（ii）. https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-0160

（iii）. http://nvd.nist.gov/nvd.cfm?cvename=CVE-2014-0160

（iv）. http://www.us-cert.gov/ncas/alerts/TA14-098A

（v）. http://jvn.jp/vu/JVNVU94401838/

（vi）. https://www.ipa.go.jp/security/ciadr/vul/20140408-openssl.html

S.S.R.C.

Shield Security Research Center

株式会社　日立システムズ
〒141-8672 東京都品川区大崎 1-2-1
http://www.hitachi-systems.com/index.html
http://www.shield.ne.jp/ssrc/index.html