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

PHPMailerにおける、リモートから任意のコードが実行可能な脆弱性（CVE-2016-10033およびCVE-2016-10045）に関する調査レポート

【概要】

PHP のライブラリである PHPMailer において、リモートより任意のコードが実行される脆弱性（CVE-2016-10033 および CVE-2016-10045）の攻撃コードが発見されました。

この脆弱性は、PHPMailer を使用してメールを送信する際に、引数として使用する Sender プロパティに対しての処理が不適切であったために生じる脆弱性です。この脆弱性を利用した攻撃が成立した場合、リモートより任意のコードが実行される危険性があります。

本脆弱性の公開から修正までの経緯は次の通りです。
本脆弱性は 2016 年 12 月 22 日に PHPMailer 5.2.17 以下を対象とする脆弱性(CVE-2016-10033)として公開されました。その後、開発元より「CVE-2016-10033」の脆弱性を修正した PHPMailer 5.2.18 がリリースされましたが、同バージョンにおいても脆弱性が完全に修正されておらず、新たに「CVE-2016-10045」が採番されました。そして、2016 年 12 月 28 日に「CVE-2016-10045」の脆弱性を修正した PHPMailer 5.2.20 がリリースされました。
本脆弱性が公開されたのが 2016 年末であったため、本脆弱性を修正できていないシステム、また、「CVE-2016-10033」の修正のみを行い、脆弱性が残存している状態で運用されているシステムに対しての注意喚起の意味込めて、今回この脆弱性（CVE-2016-10033 および CVE-2016-10045）の再現性について検証を行いました。

経緯

日時	内容
2016 年 12 月 22 日	CVE-2016-10033 公開
2016 年 12 月 24 日	PHPMailer 5.2.18 をリリース(CVE-2016-10033 を修正したバージョン。)
2016 年 12 月 26 日	CVE-2016-10045 公開
2016 年 12 月 28 日	PHPMailer 5.2.20 をリリース(CVE-2016-10045 を修正したバージョン)

【影響を受ける可能性があるシステム】

CVE-2016-10033

- PHPMailer 5.2.18 未満のバージョン

CVE-2016-10045

- PHPMailer 5.2.20 未満のバージョン

【対策案】

開発元より、この脆弱性を修正するプログラムがリリースされています。

当該脆弱性を修正した最新のバージョンを適用していただくことを推奨いたします。

【参考サイト】

CVE-2016-10033

CVE-2016-10045

JVNVU#99931177 PHPMailer に OS コマンドインジェクションの脆弱性

GitHub - PHPMailer/changelog.md

【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リクエストを送信することで、PHPMailer の脆弱性を利用して任意のコードを実行。ターゲットシステムの制御を奪取します。

今回の検証に用いたコードは、ターゲットシステム上から特定のサーバー、ポートへコネクションを確立させるよう誘導し、システム制御を奪取するものです。これにより、リモートからターゲットシステムが操作可能となります。

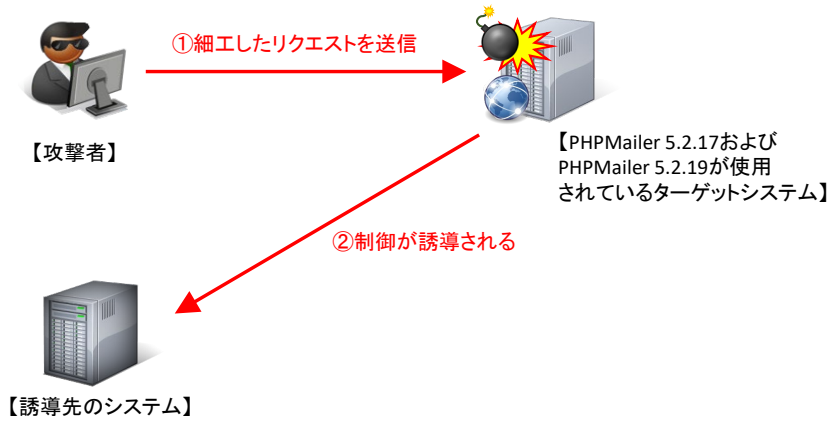
*誘導先のシステムは Linux です。

【検証ターゲットシステム】

Ubuntu 14.04 + PHP 5.5.9 + PHPMailer 5.2.17

Ubuntu 14.04 + PHP 5.5.9 + PHPMailer 5.2.19

【検証イメージ】

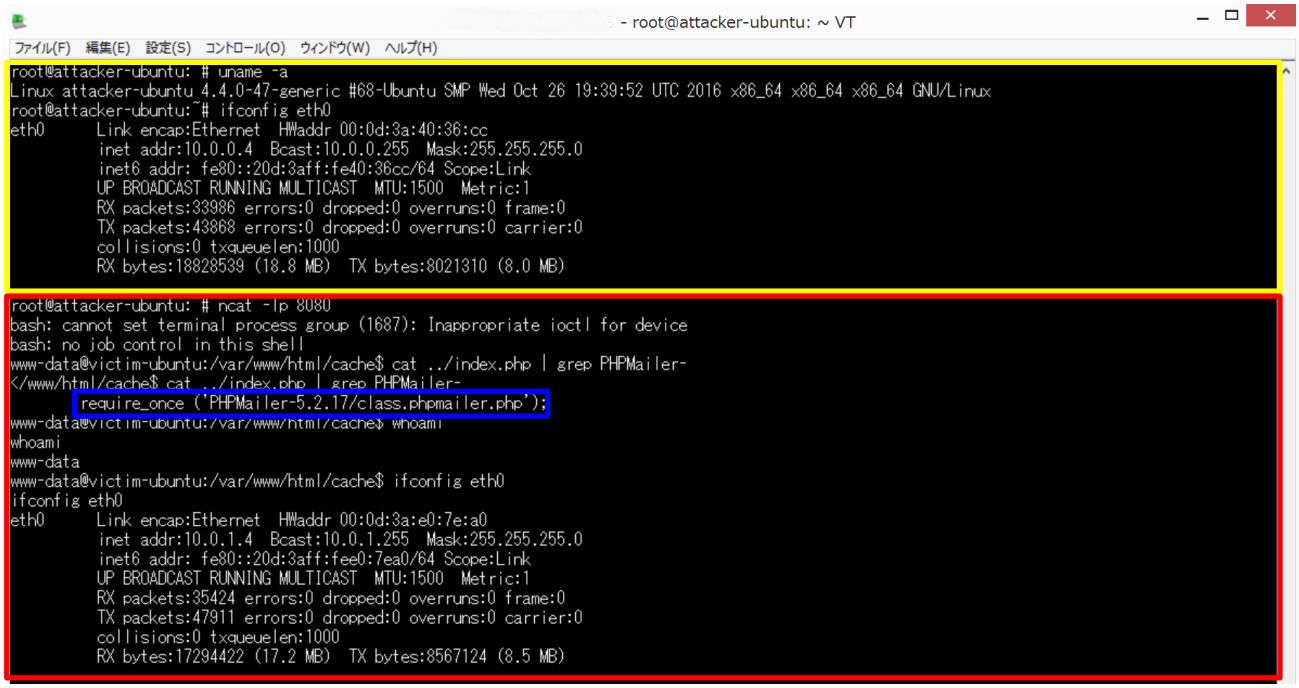


【検証結果】

下図は、誘導先のコンピュータ(Linux)の画面です。黄線で囲まれた部分は、誘導先のホストの情報です。

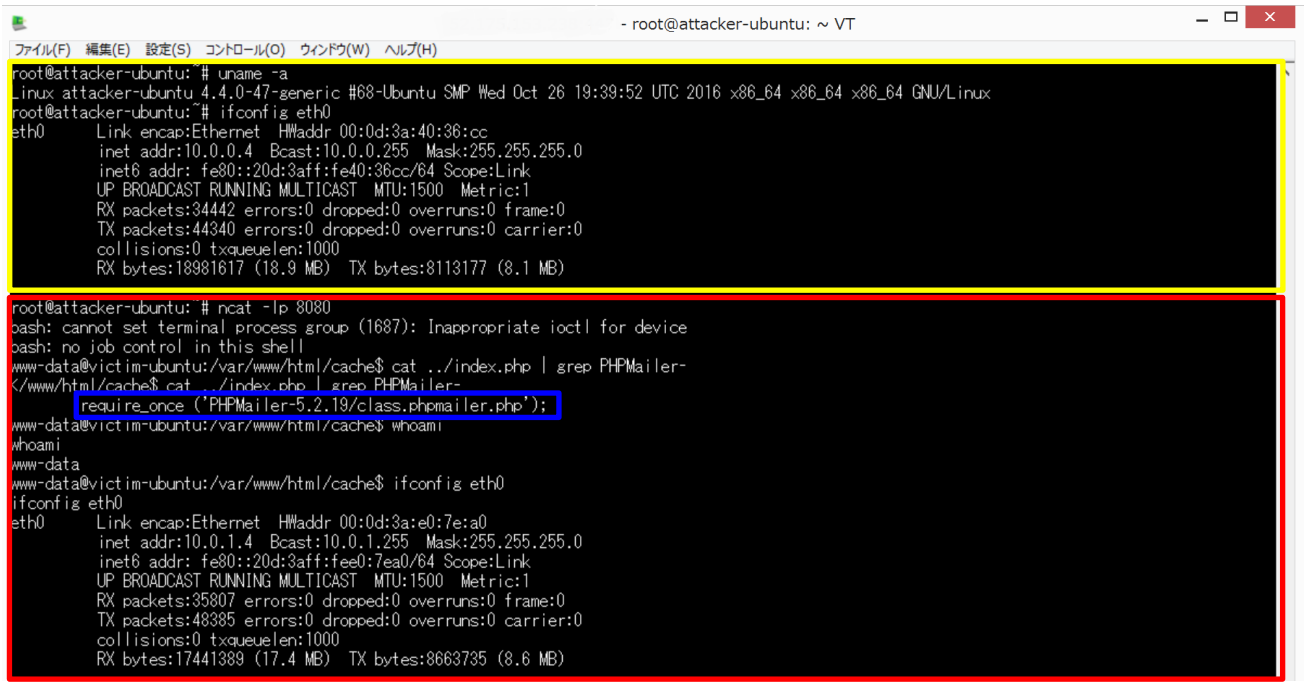
一方で、赤線で囲まれている部分は、ターゲットシステム（PHPMailer 5.2.17 および PHPMailer 5.2.19）において、ホスト名、ユーザーの情報、IP アドレスの情報を表示するコマンドを実行した結果が表示されています。
これにより、ターゲットシステムで任意のコマンドを実行することに成功したと判断できます。

PHPMailer 5.2.17 の場合



青線で囲まれている部分はターゲットシステム内、PHPMailer を使用している PHP ファイルのソースコードを一部抜粋した結果です。上記より、使用している PHPMailer のバージョンが 5.2.17 であることが分かります。

PHPMailer 5.2.19 の場合



青線で囲まれている部分はターゲットシステム内、PHPMailer を使用している PHP ファイルのソースコードを一部抜粋した結果です。上記より、使用している PHPMailer のバージョンが 5.2.19 であることが分かります。

【更新履歴】

2017 年 1 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/