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

Red Hat Enterprise Linux の DHCP クライアントパッケージの脆弱性により、リモートから任意のコードが実行可能な脆弱性（CVE-2018-1111）に関する調査レポート

【概要】

Red Hat 社の Enterprise Linux ディストリビューションの DHCP クライアントパッケージに、リモートより任意のコードが実行される脆弱性（CVE-2018-1111）の攻撃コードが発見されました。

この脆弱性は、DHCP クライアントのパッケージに含まれる NetworkManager に存在しており、NetworkManager が DHCP レスポンスを処理する際に利用するスクリプトにコマンドインジェクションを行うことが可能です。このため、攻撃者が用意した不正な DHCP サーバーへアクセスしてしまうことにより、リモートより任意のコマンドを実行することが可能です。

この脆弱性を利用した攻撃が成立した場合、リモートから任意のコマンドを実行される危険性があります。

ただし、この脆弱性が攻撃に利用されるためには、①ターゲットの IP が DHCP により割り当てられていること、②攻撃者が用意した DHCP サーバーへターゲットからの DHCP リクエストが到達し、また DHCP レスポンスを受信できること、などの条件を満たす必要があります。

本レポート作成（2018 年 5 月 18 日）時点において、各ディストリビューションベンダーより脆弱性の修正プログラムがリリースされております。脆弱性を攻撃に利用される可能性は低いと考えられますが、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、かつ脆弱性に対する攻撃が容易であることから、今回、この脆弱性（CVE-2018-1111）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】

- Red Hat Enterprise Linux Server バージョン 6, 7
- Fedora バージョン 26, 27, 28
- CentOS バージョン 6, 7
- Scientific Linux バージョン 6, 7
- Oracle Linux バージョン 6, 7 および Oracle VM バージョン 3.3, 3.4

【対策案】

本レポート作成（2018 年 5 月 18 日）時点において、各ディストリビューションベンダーより、この脆弱性を修正するプログラムはリリースされております。

当該脆弱性が修正された修正プログラムを適用していただくことを推奨します。

【参考サイト】

- DHCP Client Script Code Execution Vulnerability – CVE-2018-1111
- CVE-2018-1111 dhcp: Command injection vulnerability in the DHCP client NetworkManager integration script [fedora-all]
- CESA-2018:1454 Critical CentOS 6 dhcp Security Update
- CESA-2018:1453 Critical CentOS 7 dhcp Security Update
- SL Security Errata dhcp (SL6)
- SL Security Errata dhcp (SL7)
- Oracle Linux CVE Repository CVE-2018-1111

【検証概要】

攻撃者は、不正なレスポンスを送信する DHCP サーバーと、ターゲットシステムを制御するために用意した誘導先のホストの二台を用意します。

ターゲットシステム上で不正な DHCP レスポンスが処理されることにより、ターゲットシステムの制御を誘導先のホストが奪取するコードを実行させます。

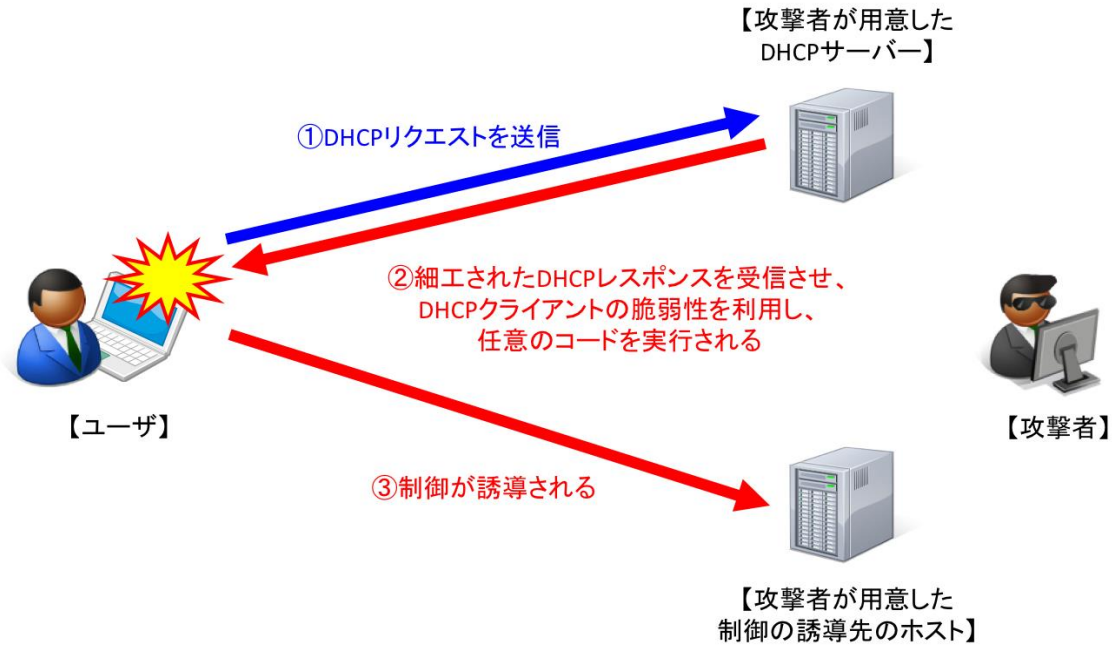
今回の検証に用いたコードは、ターゲットシステム上から特定のサーバー、ポートにコネクションを確立させるよう誘導し、システム制御を奪取するものです。これにより、リモートからターゲットシステムが操作可能となります。

*誘導先のシステムは Linux です。

【検証ターゲットシステム】

Red Hat Enterprise Linux Server 7.3

【検証イメージ】

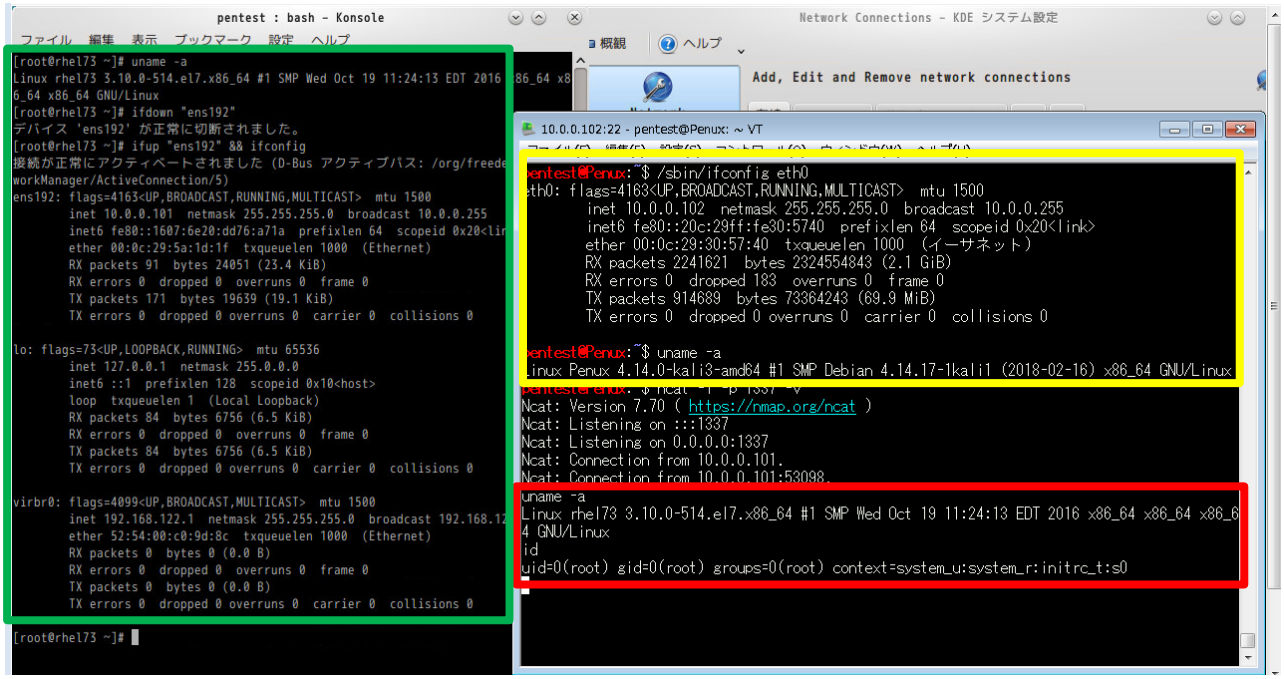


【検証結果】

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あり、緑線で囲まれた部分はターゲットシステム（Red Hat Enterprise Linux 7.3）のホストの情報、および、DHCP クライアントを実行した際の画面です。

一方で、赤線で囲まれている部分は、ターゲットシステムにおいて、ホスト名、カーネルバージョン、奪取した権限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。



【更新履歴】

2018 年 5 月 21 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/