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

Windows XP および Windows Server 2003 におけるリモートデスクトップサービスの脆弱性により、リモートから任意のコードが実行可能な脆弱性（CVE-2017-9073）に関する調査レポート

【概要】

Windows XP および Windows Server 2003 のリモートデスクトップサービス(旧ターミナルサービス)に、リモートより任意のコードが実行可能な脆弱性（CVE-2017-9073）及び、その脆弱性を利用する攻撃コードが発見されました。

本脆弱性は、スマートカード認証で使用するコンポーネント「gpkcsp.dll」内の、スマートカード情報を格納する構造体の不具合に起因するバッファオーバーフローの脆弱性で、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 Windows の SYSTEM 権限で任意のコードを実行される危険性があります。本脆弱性の影響を受けるシステムの条件は、対象システムがドメインに参加していること、リモートデスクトップサービスが動作しており、かつ同サービスにてスマートカードデバイスのリダイレクトを許可する設定になっていることです。なお、スマートカードデバイスのリダイレクトについてはデフォルトで許可する設定になっております。

また、本脆弱性は、「The Shadow Brokers」と名乗るグループによって公開された、同グループが NSA（米国家安全保障局）と関連が深いとされている、「The Equation Group」から盗んだと主張する攻撃コードの中の一つである「EsteemAudit」が悪用する脆弱性です。なお、同グループが公開した攻撃コードの中には、5 月初旬から世界中で話題となった WannaCry を拡散させるために使用されたとされる攻撃コード「EternalBlue」も含まれていました。

本レポート作成（2017 年 6 月 5 日）時点において、本脆弱性の影響を受ける可能性がある Windows XP および Windows Sever 2003 は、開発元のサポートがすでに終了 (Windows XP は 2014 年 4 月 9 日（日本時間）に、Windows Server 2003 は 2015 年 7 月 15 日（日本時間）に終了)しているため、本脆弱性を修正するプログラムがリリースされない可能性が高いこと、また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、加えて攻撃を受けた際にシステムへの影響が大きいことから、今回、この脆弱性（CVE-2017-9073）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】

- Windows XP
- Windows XP SP1
- Windows XP SP2
- Windows XP SP3
- Windows Server 2003
- Windows Server 2003 SP1
- Windows Server 2003 SP2

【対策案】

本脆弱性の影響を受ける可能性がある Windows XP および Windows Sever 2003 は、開発元のサポートがすでに終了しているため、本脆弱性を修正するプログラムはリリースされない可能性が高いと判断できます。可能な限り迅速に現在サポート中の OS へとアップデートしてください。それまでの暫定回避策としては、以下回避策のいずれかを実施することを推奨いたします。

- リモートデスクトップサービスにて「スマートカードデバイスのリダイレクトを許可しない」設定を有効にします。スマートカードを使用して認証を行っているシステムについては、代替の認証方式を検討してください。
- リモートデスクトップサービスを無効にし、代替の接続方法を検討する、もしくは対象のリモートデスクトップサービスにアクセスが可能となっている範囲を確認し、適切なアクセス元からのみアクセスが可能となるよう、アクセス元の制限を行ってください。

「スマートカードデバイスのリダイレクトを許可しない」設定を有効にする手順

「スマートカードデバイスのリダイレクトを許可しない」設定を有効にする手順は以下の通りです。

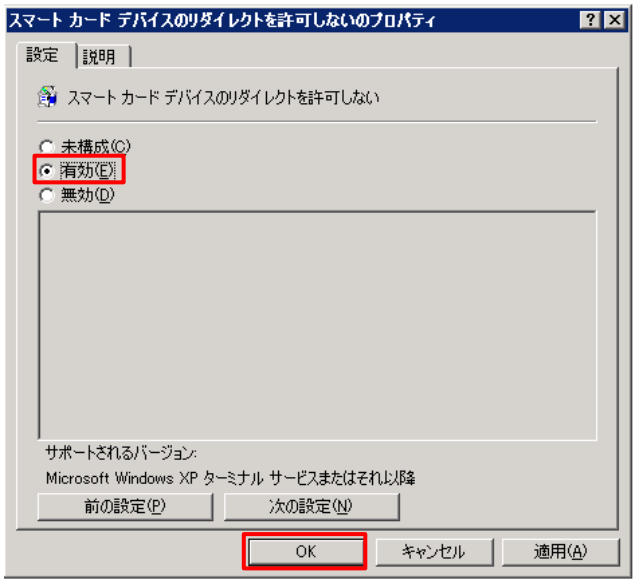
※Windows2003 での設定例です。

詳細は以下 Microsoft 社の Web サイトをご確認ください。

Device and Resource Redirection

1. Active Directory にてグループポリシーオブジェクトエディタを開き、[コンピュータの構成]-[管理用テンプレート]-[ターミナルサービス]-[クライアント/サーバー データリダイレクト]を選択。右ペインより[スマートカードデバイスのリダイレクトを許可しない]をクリックします。

2. [スマートカードデバイスのリダイレクトを許可しないのプロパティ]ウィンドウにて[有効]を選択し、[OK]ボタンをクリックします。



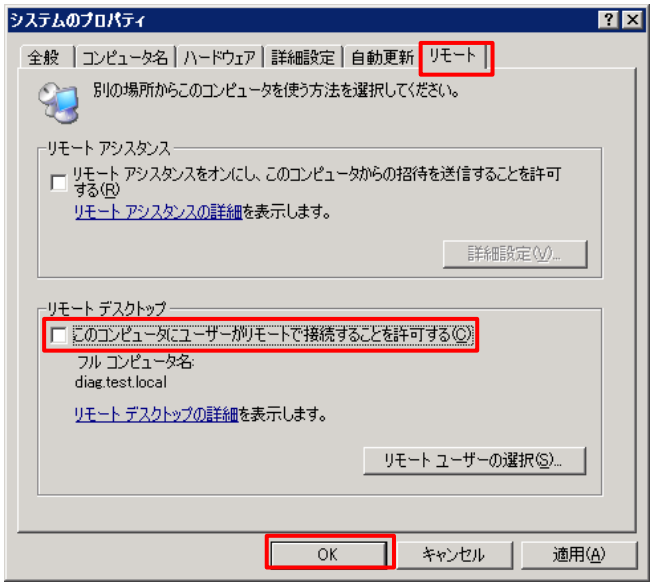
リモートデスクトップサービスを無効にする手順

リモートデスクトップサービスを無効にする手順は以下の通りです。

- システム毎に無効にする手順　※Windows2003 での設定例は下記です。

1. コントロールパネルより[システム]のアイコンを選択します。

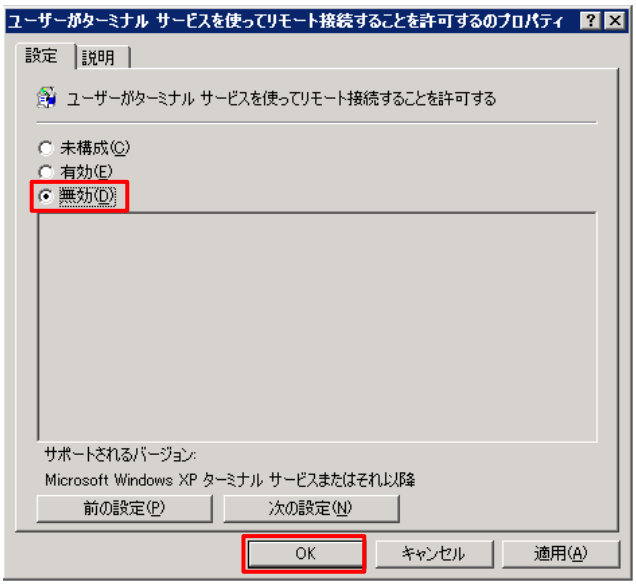
2. [システムのプロパティ]ウィンドウにて[リモート]タブを選択。[このコンピュータにユーザーがリモートで接続することを許可する]のチェックを外し、[OK]ボタンをクリックします。



- グループポリシーを使用して無効にする手順　※Windows2003 での設定例です。

1. Active Directory にてグループポリシーオブジェクトエディタを開き、[コンピュータの構成]-[管理用テンプレート]-[ターミナルサービス]を選択し、右ペインより[ユーザーがターミナルサービスを使ってリモート接続することを許可する]をクリックします。

2. [ユーザーがターミナルサービスを使ってリモート接続することを許可するのプロパティ]ウィンドウにて[無効]を選択し、[OK]ボタンをクリックします。



【参考サイト】

- CVE - CVE-2017-9073
- Protecting customers and evaluating risk
- A Dissection of the “EsteemAudit” Windows Remote Desktop Exploit

【検証概要】

攻撃者は、リモートデスクトップサービスが動作するターゲットシステムへ細工したリクエストを送信することにより、ターゲットシステムの脆弱性を利用して任意のコードを実行させます。

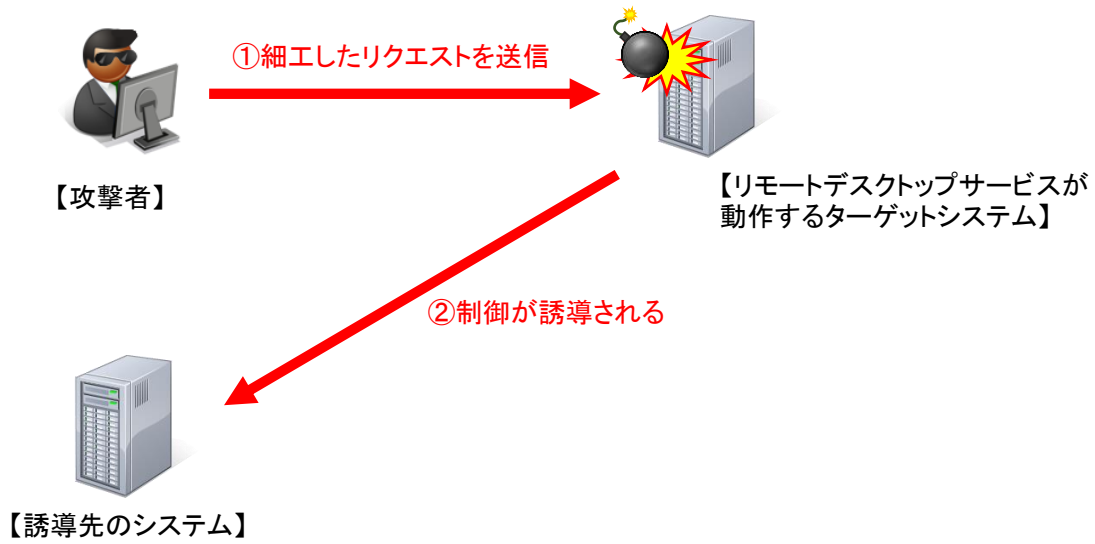
今回の検証に用いたコードは、ターゲットシステム上から特定のサーバー、ポートへコネクションを確立させるよう誘導し、システム制御を奪取するものです。これにより、リモートから Windows の SYSTEM 権限でターゲットシステムが操作可能となります。

*誘導先のシステムは Linux です。

【検証ターゲットシステム】

Windows Server 2003

【検証イメージ】

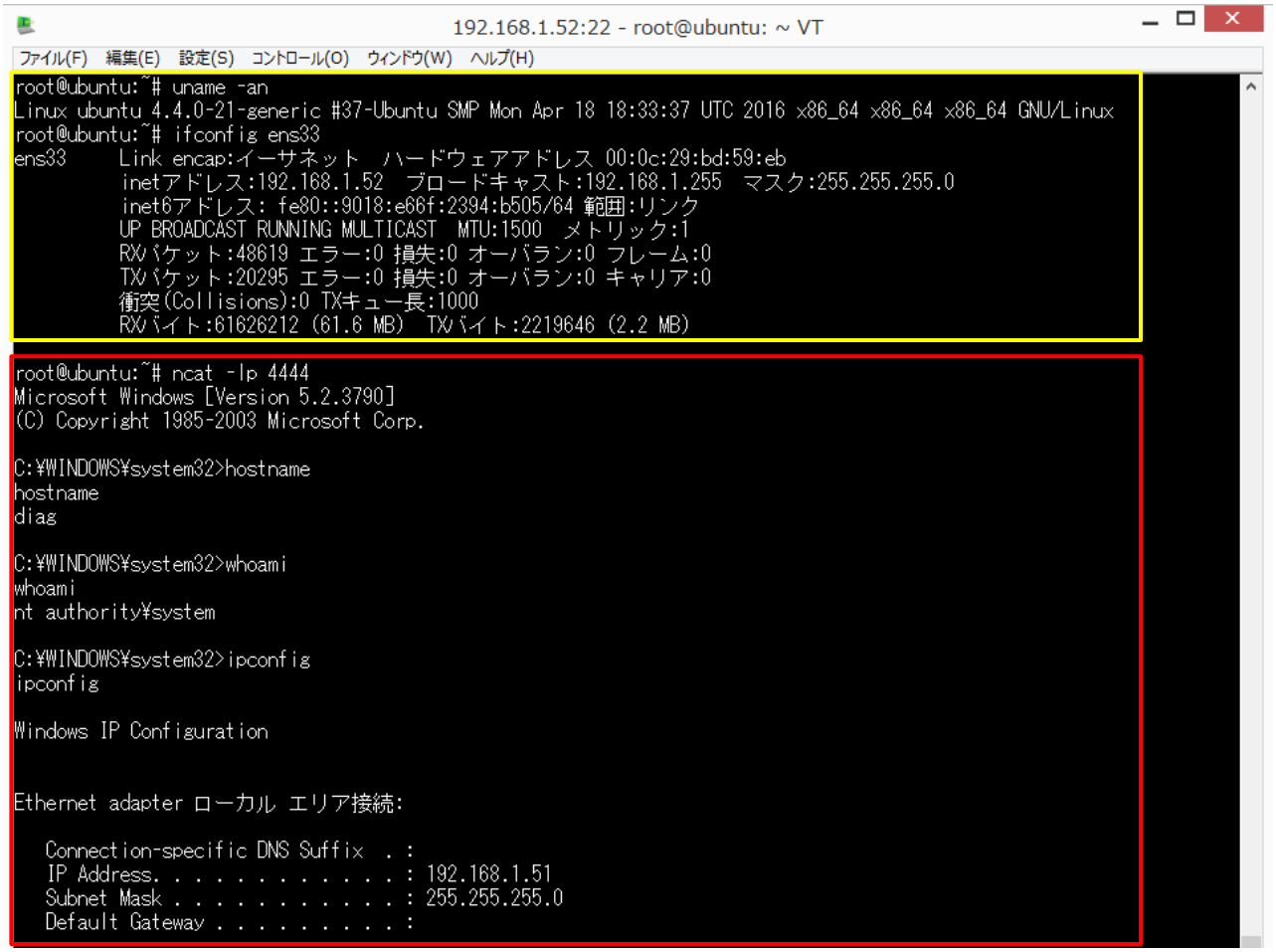

①細工したリクエストを送信
【攻撃者】
【リモートデスクトップサービスが
動作するターゲットシステム】
②制御が誘導される
【誘導先のシステム】

【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(Windows Server 2003)において、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。



【更新履歴】 2017 年 6 月 5 日 ： 初版公開

【本レポートに関するお問い合わせは下記まで】

▼報道関係者様からのお問い合わせ

ソフトバンク･テクノロジー株式会社 管理本部 経営企画部 齊藤、吉田、菅

TEL:03-6892-3063 メールアドレス:sbt-pr@tech.softbank.co.jp

▼お客様からのお問い合わせ

下記フォームよりお問い合わせください。

https://info.softbanktech.jp/public/application/add/508

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/