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 の Kerberos 認証の脆弱性により、権限昇格が行える脆弱性（CVE-2014-6324）に関する調査レポート

【概要】

Microsoft Windows の Kerberos 認証に、リモートから任意のドメインアカウントへ権限昇格を行える脆弱性（CVE-2014-6324）が発見されました。この脆弱性は、Kerberos 認証のチケットの署名に対する検証処理に問題があるため、署名に細工をすることによりドメインの特権ユーザーへ昇格することが可能です。

攻撃者がこの脆弱性を利用するためには、ドメインへの有効なログオン情報が必要になります。
攻撃者が何らかの方法でドメインユーザーのログオン情報を奪取できた場合、この脆弱性を利用することによりドメインの管理者権限を奪取される可能性があります。その結果、管理者権限でシステムを操作し、重要情報の改ざん、窃取されてしまうといった危険性があります。

本レポート作成（2014 年 12 月 17 日）時点において、既に Microsoft 社より 2014 年 11 月 19 日に脆弱性の修正プログラムがリリースされております。しかしながら、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 Kerberos 認証の脆弱性（CVE-2014-6324）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 Server 2003 Service Pack 2
- Windows Server 2003 x64 Edition Service Pack 2
- Windows Server 2003 with SP2 for Itanium-based Systems
- Windows Vista Service Pack 2
- Windows Vista x64 Edition Service Pack 2
- Windows Server 2008 for 32-bit Systems Service Pack 2（Server Core インストールを含む）
- Windows Server 2008 for x64-based Systems Service Pack 2（Server Core インストールを含む）
- Windows Server 2008 for Itanium-based Systems Service Pack 2
- Windows 7 for 32-bit Systems Service Pack 1
- Windows 7 for x64-based Systems Service Pack 1
- Windows Server 2008 R2 for x64-based Systems Service Pack 1（Server Core インストールを含む）
- Windows Server 2008 R2 for Itanium-based Systems Service Pack 1
- Windows 8 for 32-bit Systems
- Windows 8 for x64-based Systems
- Windows 8.1 for 32-bit Systems

- Windows 8.1 for x64-based Systems
- Windows Server 2012（Server Core インストールを含む）
- Windows Server 2012 R2（Server Core インストールを含む）

【対策案】

Microsoft 社より、この脆弱性を修正するプログラム（MS14-068）がリリースされています。
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いたします。

【参考サイト】

- CVE-2014-6324
- マイクロソフト セキュリティ情報 MS14-068 - 緊急 Kerberos の脆弱性により特権が昇格される (3011780)
- Additional information about CVE-2014-6324

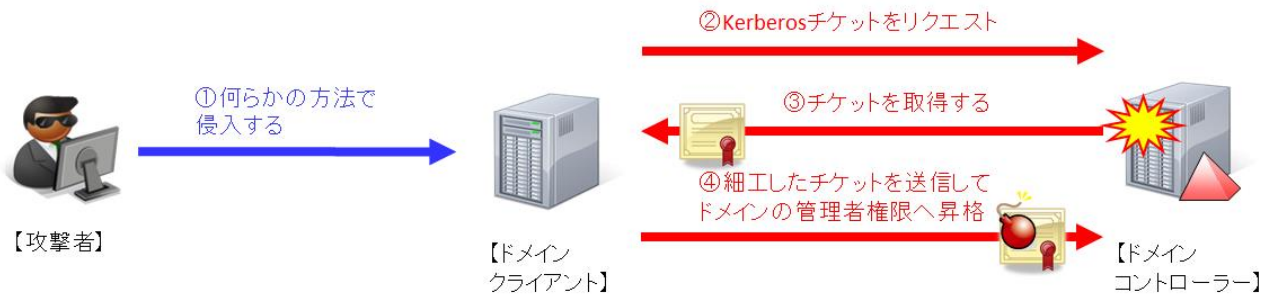
【検証概要】

ドメインに所属するクライアントへローカルの一般ユーザーでログオンした後、検証用のドメインユーザー（Domain Users グループのアカウント）の Kerberos チケットを取得します。このチケットに細工、利用しターゲットへアクセスすることで、ターゲット上にて特権で任意の操作が実行可能になるというものです。

【検証ターゲットシステム】

Windows Server 2008 R2 SP1

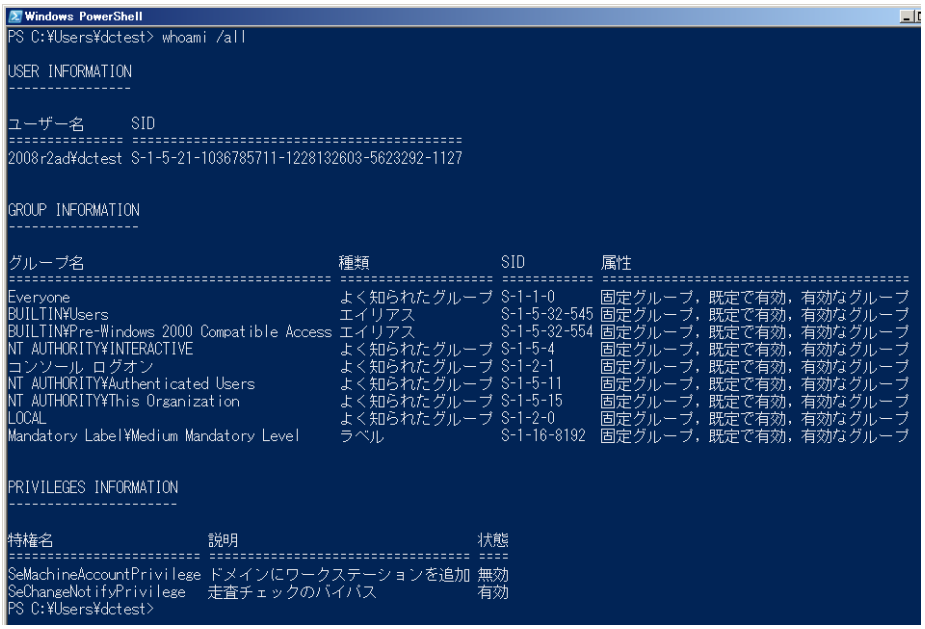
【検証イメージ】



【検証結果】

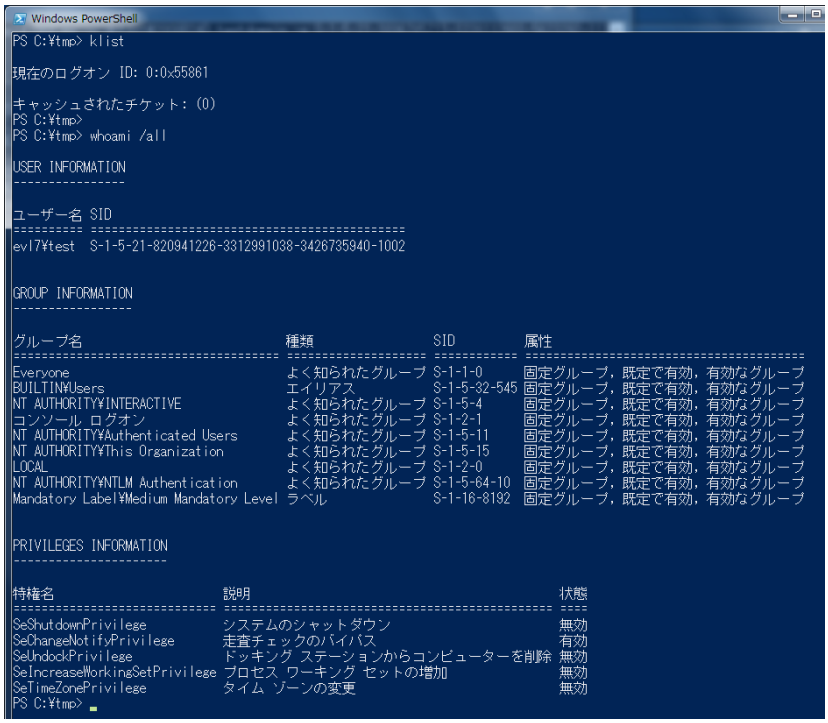
図①は、今回の検証においてターゲットシステムのコンソール画面で、ログオンしているドメインユーザーの権限を表示しています。このユーザーのチケットを取得します。

[図①]



図②は、ドメインに所属するクライアントのコンソール画面で、ログオンセッションのチケットの情報と、ログオンしているユーザーの権限を表示しています。クライアント上での操作はこのユーザーで実行しています。

[図②]



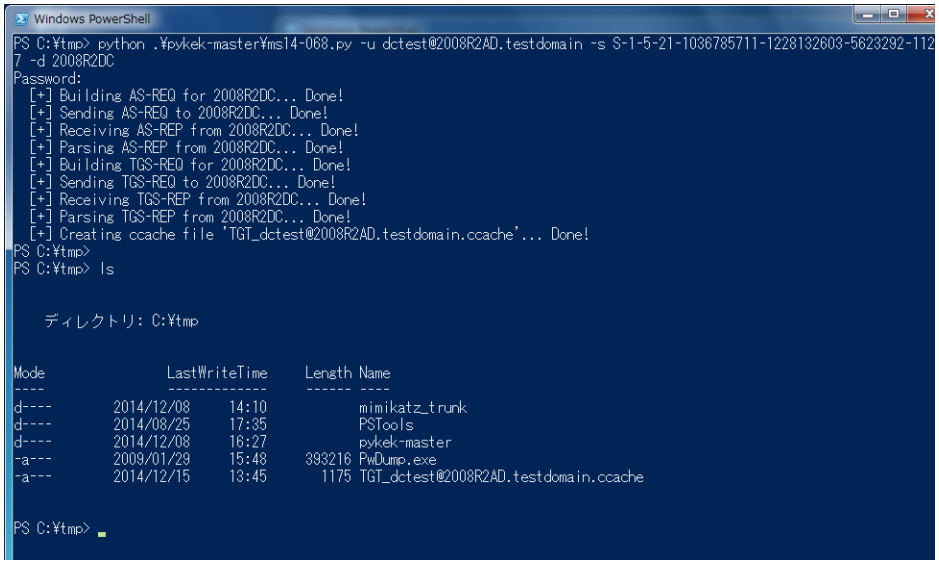
ターゲットシステムでは「dctest」ユーザーを表示しており、「Domain Users」に所属しています。クライアントでは「test」ユーザーを表示しており、ローカル（evl7）の「Users」に所属しています。

以下より検証結果を記載します。以下の図③から図⑥は MS14-068 の修正プログラムを適用する前の画像、一方で図⑦は修正プログラムを適用した後の検証結果です。

■MS14-068 適用前■

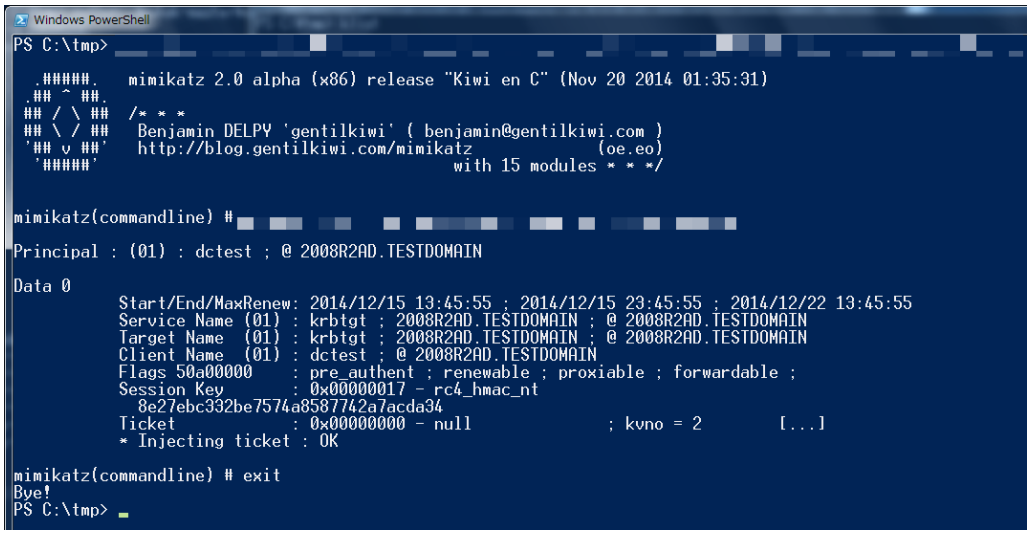
図③はドメインに所属するクライアント（Windows 7）のターミナル画面です。攻撃コードを含むスクリプトを実行することにより、ドメイン「2008R2AD.testdomain」のユーザー「dctest」の Kerberos チケットに対して、ドメインの特権を付与する細工を行います。

[図③]



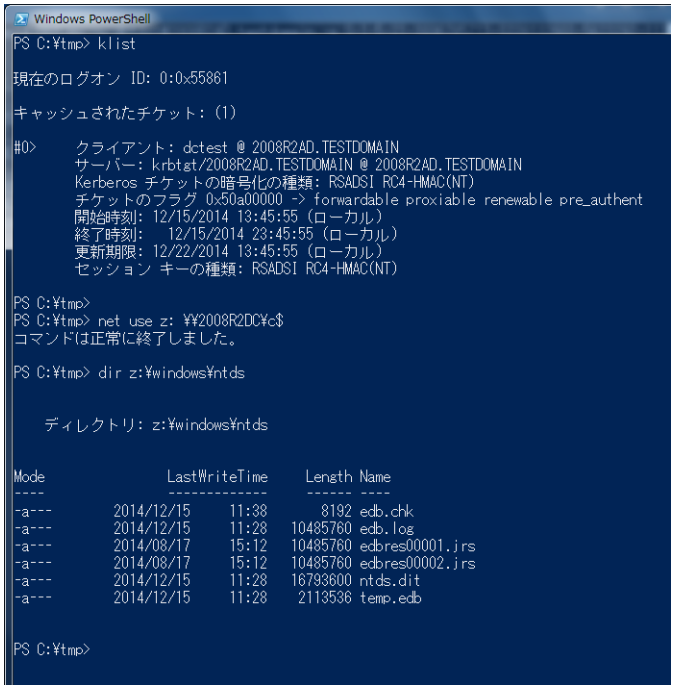
図④は、③のチケットを現在のセッションに取り込みを行ったところです。この際、このチケットのユーザー名は「dctest」であることが分かります。

[図④]



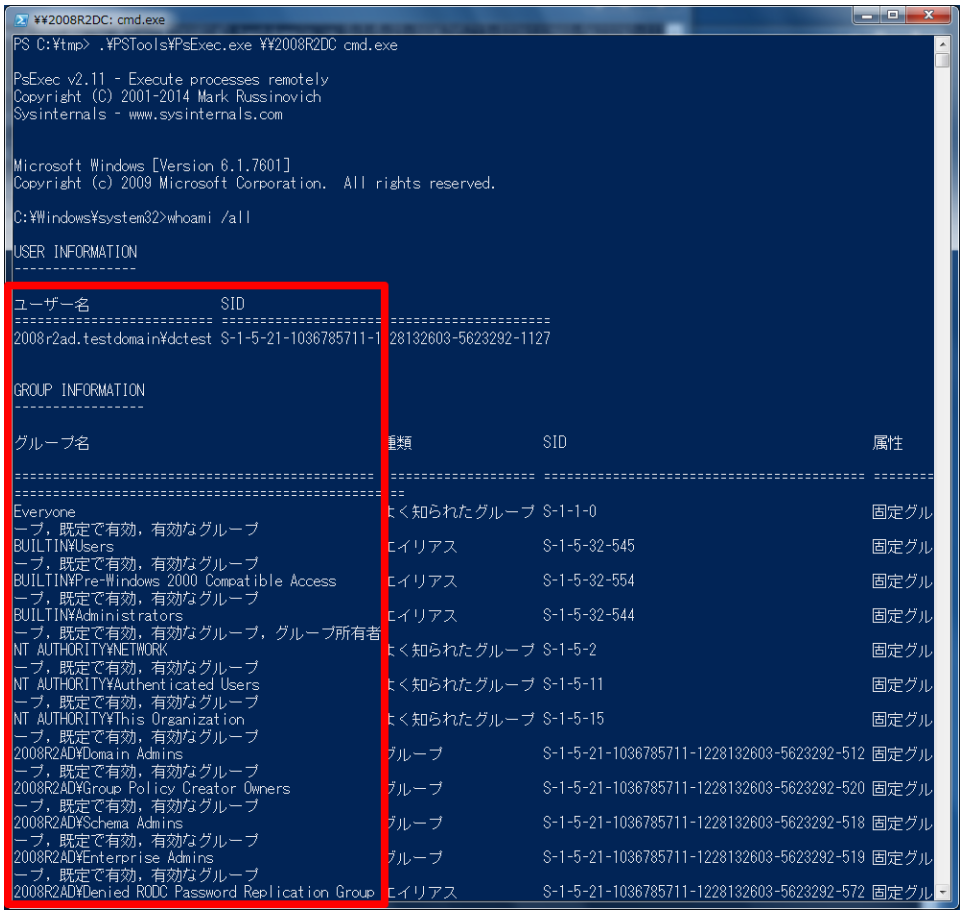
図⑤は、現在のセッションのチケットの情報を表示しています。このチケットを用いてターゲット（Windows Server 2008 R2）に対して net use による接続を試みたところです。Domain Users 権限ではアクセスできないリソースである「¥¥<ターゲット>¥c$」を、認証なしで z ドライブとしてマウントできました。

[図⑤]



図⑥は、チケットを使いターゲットのシェルを取得したところです。取得したシェルの実行権限を確認したところ、Domain Users 権限のみ与えられているはずの「dctest」ユーザーに、「Domain Admins」や「Administrators」などの権限が付与されています。このことから、この脆弱性を持つドメインコントローラーは、細工されたチケットを検証できていないことが確認できます。

[図⑥]



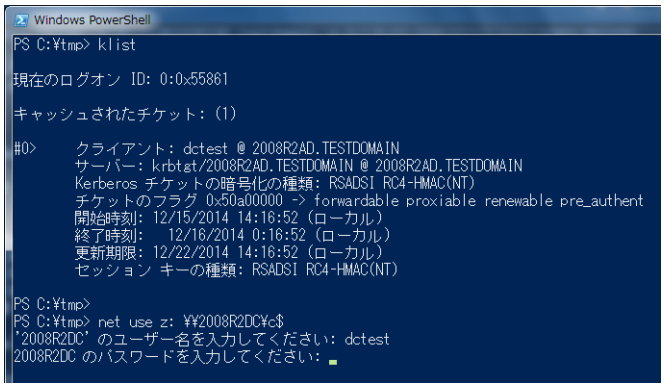
なお、Windows の Kerberos 認証では、TGT チケットにはデフォルトで 10 時間の有効期限が設定されています。
この期限内では、TGT チケットを取得されたユーザーのパスワードを変更しても、攻撃者はログオンすることが可能です。

■MS14-068 適用後■

図③から図④までと同じ手順で進めた後、図⑦では、現在のセッションにチケットがキャッシュされていることを確認しています。

次に、修正プログラム適用前の検証と同様にチケットを用いてターゲット（Windows Server 2008 R2）に対して net use による接続を試みていますが、MS14-068 を適用した後は適用前と挙動が異なり、ドメインのリソースへのアクセスに認証が求められるようになります。脆弱性を修正するプログラム適用後は、細工されたチケットを用いてドメインのリソースにアクセスできなくなっていることが分かります。
この脆弱性の修正プログラム（MS14-068）を適用していただくことにより、ドメインコントローラーはチケットを検証するようになったことが確認されました。

[図⑦]



【イベントログへの記録】

■Windows Server 2003 の場合■

この脆弱性の攻撃コードが Windows Server 2003 でも利用可能なことを確認しました。

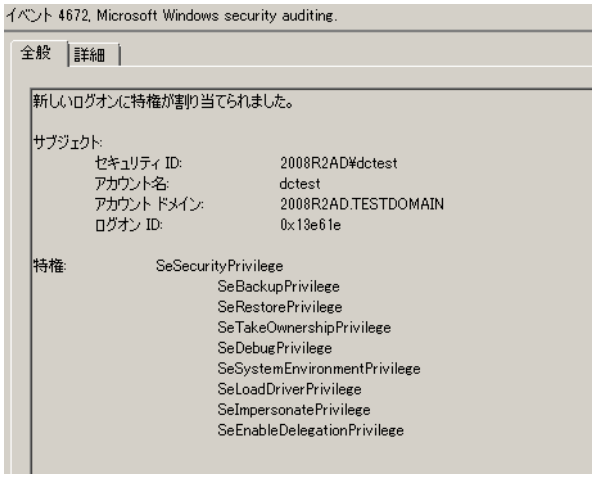
Windows Server 2003 において、MS14-068 を未適用の場合で特権の昇格の攻撃が成功した場合、Windows のシステムログ ID576 を確認することにより、不審な挙動を検出することが出来ます。脆弱性を利用したリクエストが行われた場合、ログオンユーザーに対して特権が与えられるログが記録されます。以下の例では Domain Users 権限である「diag」に対して特権が与えられていることが確認できます。

このログを取得するためには、使用しているポリシーを選択し、以下の設定を行います。

キー	コンピューターの構成¥Windows の設定¥セキュリティの設定¥ローカルポリシー¥監査ポリシー¥
サブカテゴリ	特権使用の監査

■Windows Server 2008 以降の場合■

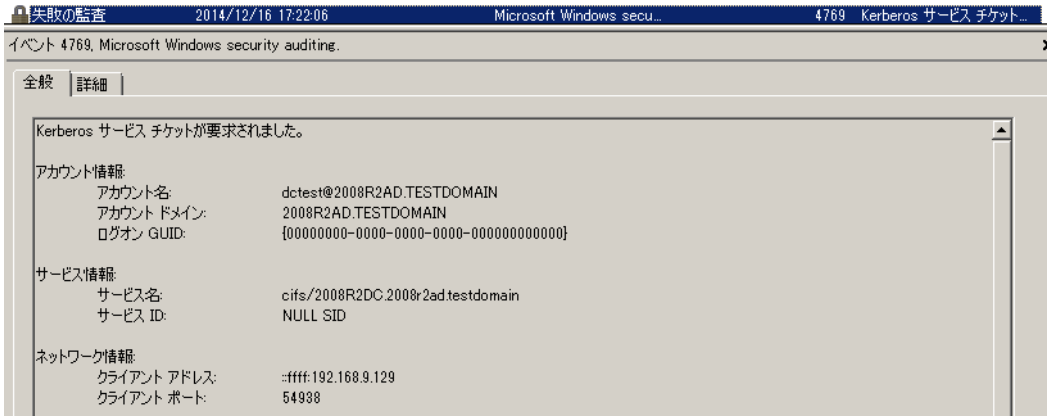
MS14-068 を未適用の場合で特権の昇格の攻撃が成功した場合、Windows のシステムログ ID4672 を確認することにより、不審な挙動を検出することが出来ます。脆弱性を利用したリクエストが行われた場合、ログオンユーザーに対して特権が与えられるログが記録されます。以下の例では Domain Users 権限である「dctest」に対して特権が与えられていることが確認できます。



このログを取得するためには、グループポリシーの管理から使用しているポリシーを選択し、以下の設定を行います。

キー	コンピューターの構成¥ポリシー¥Windows の設定¥セキュリティの設定¥監査ポリシーの詳細な構成¥監査ポリシー¥特権の使用¥
サブカテゴリ	重要な特権の使用の監査

MS14-068 を適用済みの場合、Windows のシステムログ ID4769 を確認することにより、細工されたチケットを用いた特権のリクエストを検出することが出来ます。以下の例では dctest ユーザーとしての特権のリクエストを却下したことが確認できます。



このログを取得するためには、グループポリシーの管理から使用しているポリシーを選択し、以下の設定を行います。

キー	コンピューターの構成¥ポリシー¥Windows の設定¥セキュリティの設定¥監査ポリシーの詳細な構成¥監査ポリシー¥アカウントログオン
サブカテゴリ	Kerberos サービスチケット操作の監査

更新履歴

2015 年 4 月 8 日 : 【イベントログへの記録】に Windows Server 2003 についての文章を追記

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/