NTTデータ先端技術株式会社

Microsoft Windows Ancillary Functionドライバーにおける権限昇格可能な脆弱性（CVE-2011-2005）に関する検証レポート

2011/12/9
NTT データ先端技術株式会社
辻　伸弘
小松　徹也

【概要】

Microsoft 社の Windows Ancillary Function ドライバーに、権限昇格が可能な脆弱性（CVE-2011-2005）が発見されました。
この脆弱性は、afd.sys ドライバーがユーザーモードからデータを受け取るときに、入力を正しく検証しないことが原因となります。このため、細工したアプリケーションを実行した際に、権限昇格を引き起こす可能性があります。

想定される被害としては、奪取されたユーザ権限による情報取得、改ざん、または、ワームやスパイウェアなどの悪意あるプログラムをシステム内にインストールされることが考えられます。

今回、脆弱性の再現性について検証を行いました。

【影響を受けるとされているアプリケーション】

影響を受ける可能性が報告されているのは次の通りです。

- Windows XP Service Pack 3
- Windows XP Professional x64 Edition Service Pack 2
- Windows Server 2003 Service Pack 2
- Windows Server 2003 x64 Edition Service Pack 2
- Windows Server 2003 with SP2 for Itanium-based Systems

【対策案】

Microsoft 社より、この脆弱性を修正するプログラム（MS11-080）が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。

本脆弱性はシステムに一般ユーザでログインできることが前提条件となります。そのため、今一度、脆弱なパスワードが設定されているリモートログイン可能なユーザがシステム上に存在しないか確認し、存在する場合は、強固なパスワードに変更することが推奨されます。また、不要なユーザが存在する場合には直ちに削除するといった回避策を講じることが推奨されます。
ただし、正規のユーザによる攻撃、つまり、内部犯行を行われた場合には、上記対策は回避策とはなりません。

【参考サイト】

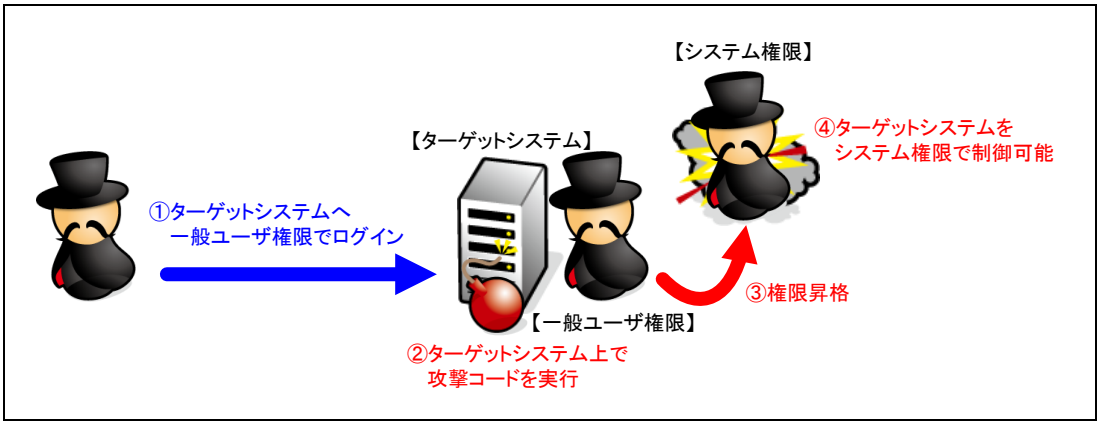
CVE-2011-2005
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-2005

マイクロソフト セキュリティ情報 MS11-080 - 重要
Ancillary Function ドライバーの脆弱性により、特権が昇格される (2592799)
http://technet.microsoft.com/ja-jp/security/bulletin/ms11-080

NTTデータ先端技術株式会社

【検証イメージ】

【CVE-2011-2005】



【検証ターゲットシステム】

Windows XP SP3

【検証概要】

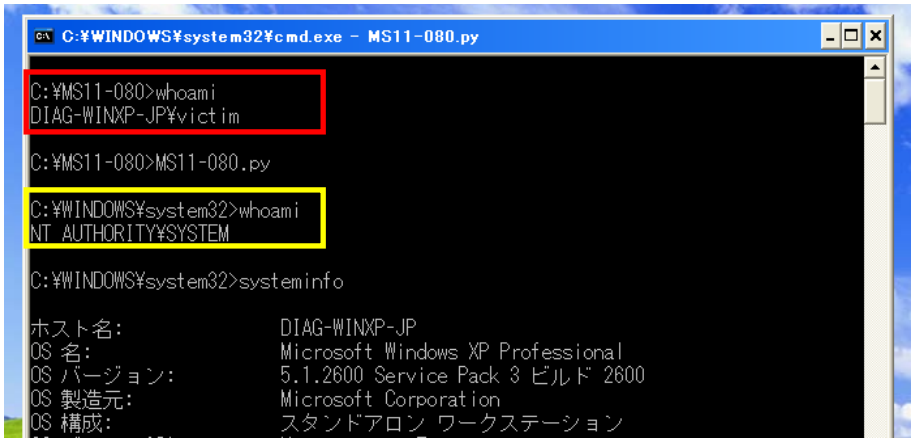
ターゲットシステムに victim ユーザでログインし、Ancillary Function ドライバーの脆弱性を利用した攻撃コードを実行することで、権限昇格させます。
これにより、ターゲットシステムをシステム権限で操作可能となります。

※本脆弱性は、ターゲットシステムに一般ユーザでログインできることが前提条件です。

【検証結果】

下図の赤線で囲まれている部分は、ターゲットコンピュータに victim ユーザでログインしている情報を表しています。黄色線で囲まれている部分は、攻撃コード実行後、ターゲットシステムにおいて、システム権限「NT AUTHORITY¥SYSTEM」に昇格している情報を表しています。これにより、システム権限でのコマンド実行が可能となり、システム権限の奪取に成功したと言えます。

ターゲットシステムの制御の奪取に成功した画面



NTTデータ先端技術株式会社

＊各規格名、会社名、団体名は、各社の商標または登録商標です。

【お問合せ先】
NTT データ先端技術株式会社
セキュリティ事業部　営業担当　営業企画グループ
TEL：03-5425-1954
http://security.intellilink.co.jp/