NTTデータ・セキュリティ株式会社

Windows のヘルプとサポートセンターの脆弱性（CVE-2010-1885）に関する検証レポート

2010/6/15
NTT データ・セキュリティ株式会社
辻 伸弘

【概要】

Windows のヘルプとサポートセンター（helpctr.exe）のエスケープシーケンス処理(UrlUnescape 関数)に脆弱性が存在します。
Windows には URL シェル拡張として「hcp://」を用いることで Web ページから Windows 内の Microsoft ヘルプサポートセンターに直接リンク可能な機能が用意されています。この拡張機能は、信頼される文書のみを操作可能にするホワイトリストが含まれていますが、そのホワイトリストが迂回可能な脆弱性が発見されました。

この脆弱性により、細工された Web ページの閲覧などで、ローカルユーザと同じ権限が奪取される危険性があります。想定される被害としては、ローカルユーザ権限での情報取得、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（CVE-2010-1885）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システム】

- Windows XP SP2 及び SP3
- Windows XP Professional x64 Edition SP2
- Windows Server 2003 SP2
- Windows Server 2003 x64 Edition SP2
- Windows Server 2003 with SP2 for Itanium-based Systems

【対策案】

このレポート作成現在（2010 年 6 月 15 日）修正プログラムはリリースされておりません。
Microsoft 社は、回避策として、HCP プロトコルの登録解除を提示しています。

「マイクロソフト セキュリティ アドバイザリ (2219475)」の「回避策」を参照ください。
http://www.microsoft.com/japan/technet/security/advisory/2219475.mspx

回避策の影響として、「hcp://」を使用するすべてのローカルの正当なリンクが解除されるため、コントロールパネル内のリンクが機能しなくなる可能性などが挙げられます。

【参考サイト】

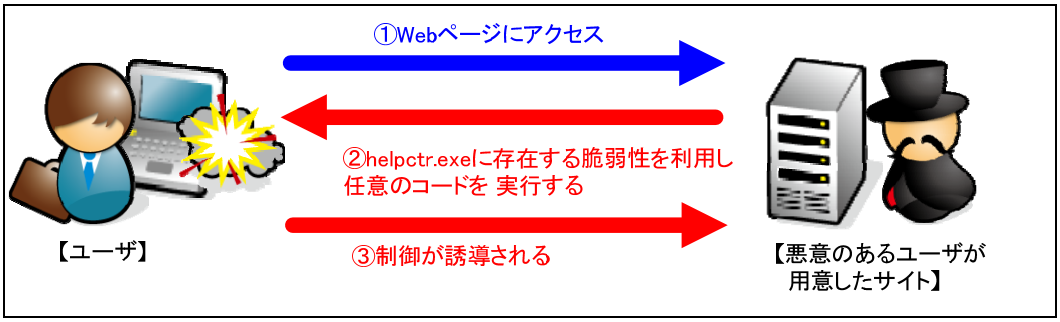
マイクロソフト セキュリティ アドバイザリ (2219475)
Windows のヘルプとサポート センターの脆弱性により、リモートでコードが実行される
http://www.microsoft.com/japan/technet/security/advisory/2219475.mspx

JVNVU#578319 Microsoft Windows Help and Support Center に脆弱性
http://jvn.jp/cert/JVNVU578319/index.html

CVE-2010-1885
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-1885

NTTデータ・セキュリティ株式会社

【検証イメージ】



【検証ターゲットシステム】

Windows XP SP3（2010 年 6 月 15 日時点にリリースされているすべての修正プログラムを適用済み）

【検証概要】

ターゲットシステムに、Web ブラウザを通じて、細工したサイトをロードさせることで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、ポートへコネクションを確立させるよう誘導し、システムの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を操作可能となります。
** 誘導先のシステムは Debian 5.04 です。*

【検証結果】

下図の赤線で囲まれている部分の示すように、誘導先のコンピュータ（Debian 5.04）上にターゲットシステム（Windows XP）のプロンプトが表示されています。
これにより、ターゲットシステムの制御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

＊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・セキュリティ株式会社
企画部　広報グループ
TEL：03-5425-1954
http://www.nttdata-sec.co.jp/