

Cisco Security Agent および Windows アニメーションカーソルにおけるスタック オーバーフローの脆弱性 (ANI ゼロデイ) エクスプロイト

概要

Microsoft Windows Vista、NT、2000、2003、XP の各オペレーティング システムにおいて、アニメーション カーソル ファイル(.ANI)に脆弱性が発見されています。この脆弱性が悪意のある Web ページまたは HTML 形式の E メール メッセージによって攻撃されると、ログイン ユーザの権限を使用したリモートでのコード実行が可能になります。¹

このエクスプロイトで注目される点は、2 年以上前(2005 年 1 月)に MS05-002のパッチで修正された脆弱性を攻撃するものと本質的に同じであることです。当時 Microsoft 社は修正プログラムを公開しましたが、これは完全なものではありませんでした。このパッチでは、ファイル内の最初のカーソルの長さを調べて、その長さが正しくない場合に処理を拒否します。今回のエクスプロイトは単純に、同一ファイル内で最初のカーソル(適正な形式)の後ろに 2 番目のカーソル(不正な形式)を付け加えるものです。Microsoft Vista など現在運用されているオペレーティングシステムは、この問題のあるコードを継承しているため、Vista においても 2 年前の脆弱性をかかえていることになります。

この脆弱性を悪用したさまざまな攻撃がすでに回っています。シスコではエクスプロイト ファイルを入手し、Cisco Security Agent のデフォルトのセキュリティ ポリシー設定を使用することで、これらのエクスプロイトを阻止する効果があることを確認しました。現在サポートされている Cisco Security Agent 4.5.x、5.0.x、5.1.x、5.2.x の各バージョンはすべて、現在までに確認されているエクスプロイトに対して有効に機能します。

脆弱性の詳細情報

この脆弱性の詳細情報は、Microsoft 社¹ および Computer Incident Response Team(CERT)² が文書で公開しています。

アニメーション カーソルは、マウス ポインタの表示場所に 1 つのイメージではなく一連のフレームを連続的に表示する機能で、短いアニメーションが繰り返されます。アニメーション カーソル機能は拡張子 .ani のファイルとして提供されますが、Windows Explorer では、.ani、.cur、.ico など、何種類かの別のファイル拡張子でも ANI ファイルとして処理されます。スタック バッファ オーバーフローの脆弱性は、Microsoft Windows が不正な形式のアニメーション カーソル ファイルを処理する際に、ANI ヘッダに指定されているサイズを適切に確認できない点にあります。

攻撃者は特殊な細工のある Web ページを作成することにより、この脆弱性を悪用しようとします。また、特殊な細工のある E メール メッセージを作成して、対象のシステムに送信する場合もあります。Web ページを閲覧する、または特殊な細工のあるメッセージをプレビューするか読む、あるいは特殊な細工のある Eメールの添付ファイルを開くと、攻撃者は侵入したシステムでコードの実行

¹ Microsoft: <http://www.microsoft.com/technet/security/advisory/935423.mspx>

² CERT Advisory: <http://www.kb.cert.org/vuls/id/191609>

が可能になります。アニメーションカーソルは一般的に拡張子 .ani に関連付けられていますが、このファイルタイプでなくても攻撃を成功させることができます。

Cisco Security Agent によるエクスプロイトの阻止

Cisco Security Agent のデフォルトポリシーには複数のルールが含まれており、エクスプロイトによる被害を回避することができます。こうした保護を実行するために Cisco Security Agent のバイナリを更新したり、デフォルト設定を変更する必要はありません。

デフォルトのセキュリティポリシーを適用した Cisco Security Agent では、次のアクションがブロックされることが確認されています。

- バッファオーバーフローによる、バッファからのシステム機能の実行
- 最近ダウンロードされたアプリケーションによるシステムファイルの修正
- システムファイルの修正
- ネットワークプロセスによるコマンドシェルの実行
- Windows プロセスによるキーストロークのキャプチャ
- コードの挿入

図 1 にこのテスト結果を示します。

図 1 Cisco Security Agent のデフォルト設定による ANI ゼロデイエクスプロイトの阻止 (Cisco Security Agent 5.2 でテストを実行)

123	4/2/2007 10:56:54 AM	metasploitxp	Notice	TESTMODE: The process 'C:\WINDOWS\winxp.exe' (as user NT AUTHORITY\SYSTEM) attempted to access a resource which would have resulted in the user being asked the following question. 'The process C:\WINDOWS\winxp.exe is attempting to inject code into the process <clb>. Do you wish to allow this?' Details: Rule 189 Wizard	Find Similar #
122	4/2/2007 10:56:54 AM	metasploitxp	Notice	TESTMODE: The process 'C:\WINDOWS\winxp.exe' (as user NT AUTHORITY\SYSTEM) attempted to access a resource which would have resulted in the user being asked the following question. 'The process C:\WINDOWS\winxp.exe is attempting to capture keystrokes. Do you wish to allow this?' Details: Rule 184 Wizard	Find Similar #
121	4/2/2007 10:56:51 AM	metasploitxp	Notice	TESTMODE: The process 'C:\WINDOWS\system32\cmd.exe' (as user METASPLOITXP\Administrator) attempted to access a resource which would have resulted in the user being asked the following question. 'The process C:\WINDOWS\system32\cmd.exe is attempting to modify the system file C:\WINDOWS\RAV2007.BAT. Do you wish to allow this?' Details: Rule 61 Wizard	Find Similar #
120	4/2/2007 10:56:50 AM	metasploitxp	Alert	TESTMODE: The current application 'C:\Documents and Settings\Administrator\Local Settings\Temporary Internet Files\Content.IE5\GRU1YDSB\down[1].exe' (as user METASPLOITXP\Administrator) attempted to execute the new application 'C:\WINDOWS\system32\cmd.exe'. The operation would have been denied. Details: Rule 451 Wizard	Find Similar #
119	4/2/2007 10:56:49 AM	metasploitxp	Notice	TESTMODE: The process 'C:\Documents and Settings\Administrator\Local Settings\Temporary Internet Files\Content.IE5\GRU1YDSB\down[1].exe' (as user METASPLOITXP\Administrator) attempted to access a resource which would have resulted in the user being asked the following question. 'The process C:\Documents and Settings\Administrator\Local Settings\Temporary Internet Files\Content.IE5\GRU1YDSB\down[1].exe is attempting to modify the system file C:\WINDOWS\RAV2007.BAT. Do you wish to allow this?' Details: Rule 61 Wizard 2 similar events (same Type/Rule ID/Application) Find Similar #	Find Similar #
118	4/2/2007 10:56:49 AM	metasploitxp	Notice	TESTMODE: The process 'C:\WINDOWS\winxp.exe' (as user NT AUTHORITY\SYSTEM) attempted to access a resource which would have resulted in the user being asked the following question. 'The process C:\WINDOWS\winxp.exe is attempting to modify the system file C:\WINDOWS\winxp.DLL. Do you wish to allow this?' Details: Rule 61 Wizard	Find Similar #
117	4/2/2007 10:56:48 AM	metasploitxp	Notice	TESTMODE: The process 'C:\WINDOWS\winxp.exe' (as user NT AUTHORITY\SYSTEM) attempted to access a resource which would have resulted in the user being asked the following question. 'The process C:\WINDOWS\winxp.exe is attempting to invoke a system function from a buffer. Do you wish to allow this?' Details: Rule 106 Wizard	Find Similar #
116	4/2/2007 10:56:46 AM	metasploitxp	Notice	TESTMODE: The process 'C:\Documents and Settings\Administrator\Local Settings\Temporary Internet Files\Content.IE5\GRU1YDSB\down[1].exe' (as user METASPLOITXP\Administrator) attempted to access a resource which would have resulted in the user being asked the following question. 'The process C:\Documents and Settings\Administrator\Local Settings\Temporary Internet Files\Content.IE5\GRU1YDSB\down[1].exe is attempting to invoke a system function from a buffer. Do you wish to allow this?' Details: Rule 106 Wizard 2 similar events (same Type/Rule ID/Application) Find Similar #	Find Similar #
115	4/2/2007 10:56:46 AM	metasploitxp	Notice	TESTMODE: The process 'C:\WINDOWS\system32\cmd.exe' (as user METASPLOITXP\Administrator) attempted to access a resource which would have resulted in the user being asked the following question. 'A process is attempting to invoke C:\Documents and Settings\Administrator\Local Settings\Temporary Internet Files\Content.IE5\GRU1YDSB\down[1].exe which has been recently downloaded and may be dangerous. Do you wish to allow this?' Details: Rule 454 Wizard 1 similar event (same Type/Rule ID/Application) Find Similar #	Find Similar #
114	4/2/2007 10:56:44 AM	metasploitxp	Notice	TESTMODE: The process 'C:\Program Files\Internet Explorer\iexplore.exe' (as user METASPLOITXP\Administrator) attempted to access a resource which would have resulted in the user being asked the following question. 'The process C:\Program Files\Internet Explorer\iexplore.exe is attempting to invoke a system function from a buffer. Do you wish to allow this?' Details: Rule 106 Wizard 3 similar events (same Type/Rule ID/Application) Find Similar #	Find Similar #

注: シスコでは、エージェントをテストモードにしてエクスプロイトをテストしました。テストモードでは、悪意のある動作に対して警告を発行します (ブロックはしません)。これにより、Cisco Security Agent のデフォルトポリシーがエクスプロイトを阻止するあらゆる方法について確認できます。エージェントをプロテクトモード (一般的な動作設定) にすると、最初のルールによってエクスプロイトが阻止されるため、悪意のある動作を実行する前にエクスプロイトが処理され、以降のイベントは発生しません。

テストは、Cisco Security Agent のデフォルト ポリシーを対象に実施しました。Cisco Security Agent を有効に機能させるために、バイナリまたはポリシーの更新は必要ありませんでした。つまり、文字通りの「Day Zero」保護のテストだと言えます。シスコでは、過去のエクスプロイトおよびワームの場合と同様に、バイナリまたはポリシーの更新を実行することなく、Cisco Security Agent のデフォルト設定によってエクスプロイトを阻止できることを確認しました。次のリストは、Cisco Security Agent のデフォルトのセキュリティ ポリシー設定によって阻止された、過去のワームやエクスプロイトの一部を示します。

表 1

エクスプロイト	ワーム	エクスプロイト	ワーム
Bagle	E メール ワーム	MS06-035	OS の脆弱性
BigYellow	ネットワーク ワーム	MS06-040	OS の脆弱性
Blackworm	ネットワーク ワーム	MS06-070	OS の脆弱性
Blaster	ネットワーク ワーム	MS07-014	アプリケーションの脆弱性
Bugbear	E メール ワーム	Excel hlink.dll	アプリケーションの脆弱性
Code Red	ネットワーク ワーム	MS RDS ActiveX	OS の脆弱性
Debplot	ネットワーク ワーム	MS XML Core Svs	OS の脆弱性
Fizzer	E メール ワーム	Nimda	ネットワーク ワーム
Gator/GAIN	スパイウェア	Pentagone/Gonner	E メール ワーム
Hotbar	スパイウェア	Sasser	ネットワーク ワーム
HTTP Dir Traversal	Web サーバの脆弱性	Sircam	E メール ワーム
IE Text Range	アプリケーションの脆弱性	Sobig	E メール ワーム
IE VML BO	アプリケーションの脆弱性	Storm Trojan	E メール ワーム
SQL Slammer	ネットワーク ワーム	WMF 0day	OS の脆弱性
SQL Snake	ネットワーク ワーム	Word BO	アプリケーションの脆弱性
JPEG/GDI+	マルウェア ダウンローダ	W32.Rinbot.H	ネットワーク ワーム
MyDoom	E メール ワーム	Zotob	ネットワーク ワーム

今回のエクスプロイトは、組織のコンピューティング環境およびネットワーク環境に深刻な打撃を与え、発生と変化を続ける攻撃の 1 つにすぎません。このような新しい攻撃を阻止するために重要なことは、デフォルト設定に変更を加えることなく攻撃を阻止できる能力、およびデフォルト ポリシー内のさまざまなルールによる多層型防御の 2 点を実現することです。

©2007 Cisco Systems, Inc. All rights reserved.

Cisco, Cisco Systems、およびCisco Systemsロゴは、Cisco Systems, Inc. またはその関連会社の米国およびその他の一定の国における登録商標または商標です。本書類またはウェブサイトに掲載されているその他の商標はそれぞれの権利者の財産です。

「パートナー」または「partner」という用語の使用はCiscoと他社との間のパートナーシップ関係を意味するものではありません。(0704R)

この資料に記載された仕様は予告なく変更する場合があります。



シスコシステムズ株式会社

〒107-6227 東京都港区赤坂9-7-1 ミッドタウン・タワー

<http://www.cisco.com/jp>

お問い合わせ先(シスコ コンタクトセンター)

<http://www.cisco.com/jp/go/contactcenter>

0120-092-255 (通話料無料)

電話受付時間：平日10:00～12:00、13:00～17:00

お問い合わせ先