

Cisco Security Agent および Symantec Big Yellow BotWorm エクスプロイトの阻止

概要

2006 年 12 月 15 日、新種のワーム(コード名「Big Yellow」)が検出されました。Big Yellow は、Symantec 社のリモート バッファ オーバーフロー脆弱性(2006 年 5 月 24 日に検出)を悪用しています。[1] この脆弱性は、2006 年 11 月 30 日、別の類似ワームによって悪用されていることが発表されました。

この脆弱性は、Symantec Client Security バージョン 3.0 と 3.1、および Symantec AntiVirus Corporate Edition バージョン 10.0 ~ 10.1 製品の Microsoft Windows バージョンで確認されています。2006 年 5 月の報告で、Symantec 社は、Symantec Client Security および Symantec AntiVirus Corporate Edition に、バッファ オーバーフロー脆弱性があることを確認し、脆弱なバージョンにパッチを発行しました。

この脆弱性を悪用したさまざまな攻撃がすでに出版されています。シスコシステムズはエクスプロイト ファイルを入手し、Cisco Security Agent で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。現在サポート中のバージョンである Cisco Security Agent 4.0.3.x、4.5.1.x、5.0.0.x、および 5.1.0.x は、今までに確認されているエクスプロイトを防ぐうえで効果的です。

脆弱性の詳細情報

Big Yellow ワームにより、Symantec 製品のバッファ オーバーフロー脆弱性が悪用されると、脆弱なコンピュータはウイルスに感染して、リモート制御されてしまいます。この新種の「botworm」は、脆弱性のある Symantec 製ソフトウェアを実行するコンピュータをスキャンして、侵入を試みます。[2] この脆弱性を悪用する攻撃者によって、影響を受けるシステムが完全に制御される可能性があります。攻撃者はその後、プログラムのインストール、データの閲覧/変更/削除、完全なユーザ権限を持つ新規アカウントの作成などを実行できます。

2006 年 11 月には、類似したワーム(Spybot の変種)が蔓延しました。Spybot も Big Yellow も、PC にインストールされるとシステムのバックドアを開き、Internet Relay Chat サーバに接続して、感染したコンピュータを攻撃者がリモートで制御できるようにします。Microsoft 社によれば、このようリモート制御ソフトウェアが、Windows PC に最も大きな被害をもたらすと言われています。[2]

Big Yellow の「botworm」によって悪用されている Symantec 製品のバッファ オーバーフロー脆弱性は、「COM_FORWARD_LOG」コマンドの処理中に発生するリモート管理インターフェイスの境界エラーに起因します。これが悪用されると、特別に細工された「COM_FORWARD_LOG」コマンド経由で TCP ポート 2967 へ送信されるスタックベースのバッファ オーバーフローが発生します。[3]

Cisco Security Agent によるエクスプロイトの阻止

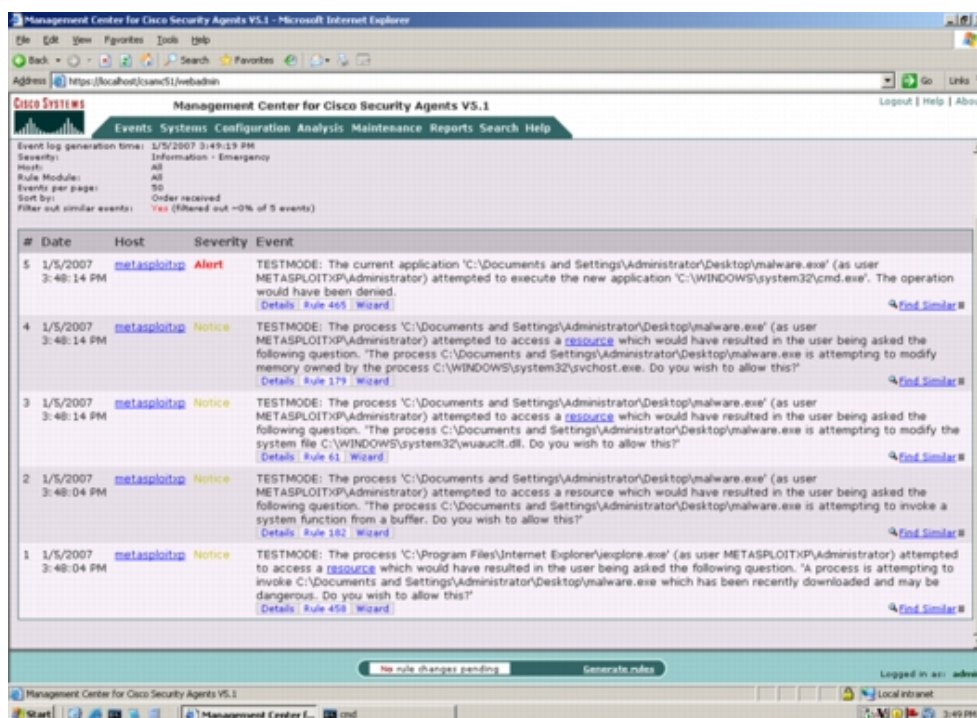
Cisco Security Agent のデフォルト ポリシーには複数のルールが含まれており、エクスプロイトによる被害を回避できます。こうした保護を実行するために、Cisco Security Agent のバイナリを更新したり、デフォルト設定を変更する必要はありません。

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、以下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。

- 信頼できないリモート アプリケーションによるシステム ファイルの修正
- 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
- 信頼できないアプリケーションの実行

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 Symantec Big Yellow Botworm エクスプロイトの阻止 (Cisco Security Agent 5.1 でテストを実行)



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、悪意のある振る舞いに対し警告を発行します (ブロックはしません)。このテストにより、Cisco Security Agent のデフォルト ポリシーを設定した状態で、エクスプロイトを阻止するすべての方法が監視されることを確認しました。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ます。エクスプロイトは悪意ある動作を実行する前に処理され、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 ポリシーに対して実施しました。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、過去のワームおよびエクスプロイトの一部です。

Bagle	E-mail worm	SQL Snake	Network worm
Blaster	Network worm	JPEG/GDI+	Malware downloader
Bugbear	E-mail worm	MyDoom	E-mail worm
Code Red	Network worm	Nimda	Network worm
Debplot	Network worm	Pentagone/Gonner	E-mail worm
Fizzer	E-mail worm	Sasser	Network worm
Gator/Gain	Spyware	Sircam	E-mail worm
Hotbar	Spyware	Sobig	E-mail worm
SQL Slammer	Network worm	Zotob	Network worm

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。

参考

[1] eEYE Digital Security: <http://research.eeye.com/html/alerts/AL20061215.html>

[2] CNET News: http://news.com.com/New+botworm+exploits+Symantec+flaw/2100-1002_3-6144282.html

[3] Secunia Advisory: <http://secunia.com/advisories/20318>

©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。(0701R)

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

〒107-0052 東京都港区赤坂2-14-27 国際新赤坂ビル東館

<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