

Cisco Security Agent および Microsoft MS06-040 に関するセキュリティ情報: Server サービスの脆弱性により、リモートでコードが実行される問題

概要

2006 年 8 月 8 日、Microsoft Windows 2000、Windows XP および XP Professional、Windows 2003 Server オペレーティング システムを対象とした、重大な脆弱性が発表されました (<http://www.microsoft.com/technet/security/bulletin/ms06-040.mspx>)。現在、この脆弱性の悪用による被害が多数報告されています。Server サービスにはリモートでのコード実行に関する脆弱性があり、この脆弱性を攻撃者に悪用された場合、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。マイクロソフト社はこのような脆弱性を持つオペレーティング システムに対し、自社 Web サイト (www.microsoft.com) で更新プログラムを公開しています。

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、こうした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

これはリモートでコードが実行される脆弱性であり、Server サービスに未チェックのバッファが含まれることが原因で生じます。Server サービスはネットワーク上で、Remote Procedure Call (RPC; リモート プロシージャ コール) のサポート、ファイル印刷のサポート、および名前付きパイプ共有を実現します。Server サービスによってローカル リソース (ディスク、プリンタなど) を共有することで、ネットワーク上の他のユーザはこれらのリソースにアクセスできます。また、Server サービスを使用すると、RPC に使用されているコンピュータと他のコンピュータ上で実行されているアプリケーションとの間で、名前付きパイプによる通信が可能になります。

この脆弱性を攻撃者に悪用された場合、影響を受けるシステムが完全にリモート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。

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 ポリシーにはバッファ オーバーフローを防止するルールが含まれており、この種の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 のバイナリまたは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。

- 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

図 1 に、このテスト結果を示します。

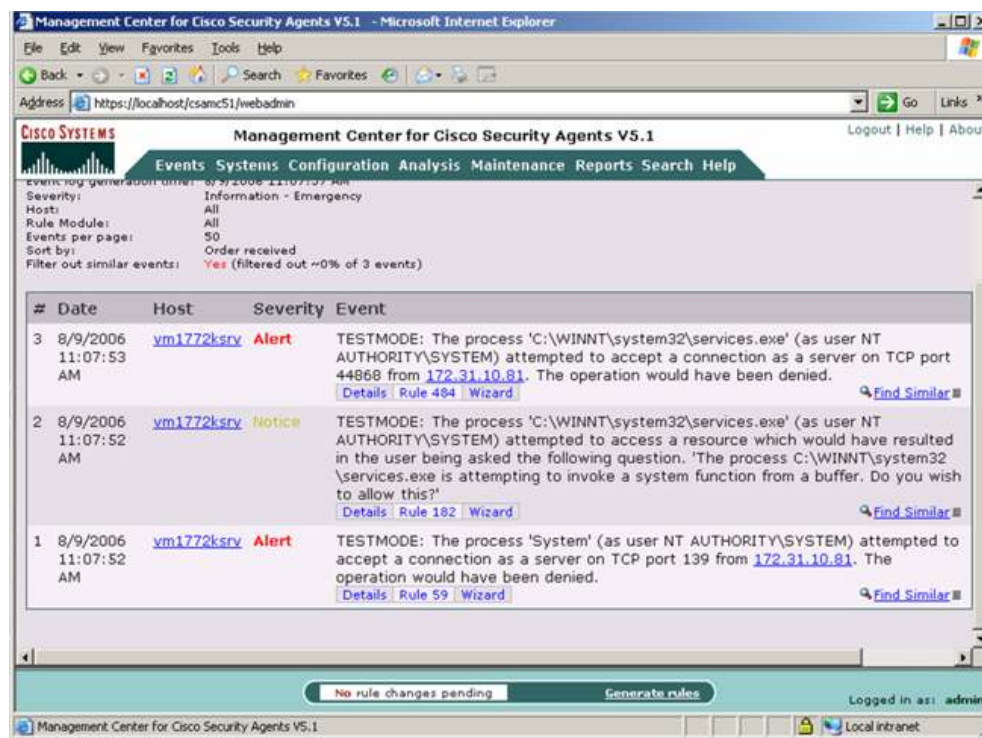
シスコでは、エージェントをテスト モードにしてエクスプロイトをテストしました。テスト モードでは、悪意ある振る舞いはブロックされません。この場合、エージェントをプロテクト モードにしたときに適用されるすべてのルールが報告されるため、Cisco Security Agent のデフォルト ポリシーでエクスプロイトを阻止する場合に使用可能なすべての方法を確認できます。エージェントをプロテクト モード（一般的な動作設定）にすると、最初のルールによってエクスプロイトが阻止されます。エクスプロイトは悪意ある動作を実行する前に処理され、以降のイベントは発生しません。

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を示します。

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
Debploit	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。このような新たな攻撃による被害を防止するために重要となるのは、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であり、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実現です。

図 1 Cisco Security Agent のデフォルト設定による Microsoft MS06-040 エクスプロイトの阻止 (Cisco Security Agent 5.1 でテストを実行)



©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