SAMPLE

Security BOSS™

xxxxxxxx 様

SecurityBOSS™ システム診断サービス

xxxx年 xx 月分 診断レポート

NTT PC COMMUNICATIONS

（株）NTT PC コミュニケーションズ

1. サマリーレポート

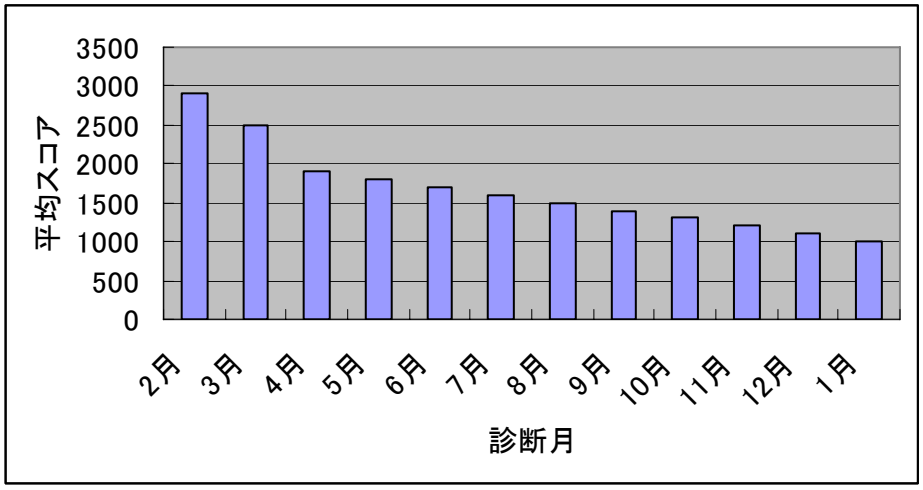
〇ネットワーク全体の診断結果

検出されたホスト数	10
スコア平均値	1000
診断結果	非常に危険

〇診断結果とホスト分布

診断結果	ホスト数	ホスト分布
非常に危険	1	10%
危険	0	0%
注意	1	10%
比較的安全	8	80%

〇平均スコアの推移



2. 検出されたホストの一覧

IP アドレス	ホスト名	OS	スコア	診断結果
192.168.0.1	HOST1	Windows XP SP2	9780	非常に危険
192.168.0.2	HOST2	Windows 4.x (Win-dows 95, Windows98, Windows NT)	200	注意
192.168.0.3	HOST3	Windows 4.x (Win-dows 95, Windows98, Windows NT)	10	比較的安全
192.168.0.4	HOST4	Windows XP (SP0 -SP2)	10	比較的安全
192.168.0.5	HOST5	Windows 4.x (Win-dows 95, Windows98, Windows NT)	0	比較的安全
192.168.0.6	HOST6	Windows 2000 SP4	0	比較的安全
192.168.0.7	HOST7	Windows 2000 SP4	0	比較的安全
192.168.0.8	HOST8	Windows 2000 SP4	0	比較的安全
192.168.0.9	HOST9	Windows 2000 SP4	0	比較的安全
192.168.0.10	HOST10	Windows 2000 SP4	0	比較的安全

3.ホスト個別レポート

3-1.ホスト 192.168.0.1

○ホスト情報

IP アドレス	192.168.0.1	ホスト名	HOST1
OS	Windows XP SP2	診断結果	非常に危険

○検出されたアプリケーション

アプリケーション名	ポート
Microsoft Windows Remote Access Connection Manager (TCP)	1025
Microsoft Windows RPC-DCOM (TCP)	135
Windows XP Direct SMB Hosting Service	445
HTTP-Based Application	5000
UPnP HTTP	5000
Windows NetBIOS Name Service	137
Windows XP NBT	139
Windows Time Service 2.x	123

○検出された脆弱性

ID	脆弱性名	ポート/プロトコル	危険度
10	MS05-043: Microsoft Windows Print Spooler Service Buffer Overflow Vulnerability	135/tcp	非常に危険
100	MS03-043: Microsoft Windows Messenger Service Buffer Overrun Vulnerability	137/tcp	非常に危険
5	MS04-007: Microsoft Windows ASN.1 Library Integer Handling Vulnerability	445/tcp	危険
20	MS04-011: Microsoft Windows Logon Process Remote Buffer Overflow Vulnerability	445/tcp	危険
40	NetBIOS Name Table	137/tcp	比較的安全
30	SMB Null Session Enumeration	137/tcp	比較的安全
15	DCE RPC mapper available	135/tcp	比較的安全

4. 各脆弱性の解説

4-1 脆弱性 ID 10

〇脆弱性情報

脆弱性名	MS05-043: Microsoft Windows Print Spooler Service Buffer Overflow Vulnerability
カテゴリ	DOS
危険度	非常に危険
リスクレベル	Remote Privileged
スキルレベル	Windows GUI
CVE	CVE-2005-1984

〇脆弱性の内容

解説

Microsoft の Windows オペレーティングシステムには、バッファオーバーフローがリモートで悪用される脆弱性があり、攻撃者に任意コードの実行を許してしまう可能性があります。

バッファオーバーフローの脆弱性は Windows の複数のバージョンに含まれている Print Spooler Service 内で発見されています。この脆弱性のリモートからの悪用は、相応のパーミッションを持つローカルユーザがプリンタを共有するか、共有プリンタに接続を試みない限り、発生しません。共有プリンタが存在せず、ローカルユーザがリモートプリンタに接続しようとしない場合、この脆弱性を悪用するには、攻撃者が有効な認証情報を使ってログオンしなくてはなりません。

任意コードの実行が失敗に終わった場合でも、DOS（サービス拒否）状態が発生してしまうことに注意してください。

脆弱性が存在する Microsoft 製品は次のとおりです。

- Microsoft Windows 2000 Service Pack 4
- Microsoft Windows 2000 Service Pack 1
- Microsoft Windows 2000 Service Pack 2
- Windows Server 2003
- Itanium システム向け Windows Server 2003

解決策

ベンダからこの脆弱性を修正するパッチがリリースされています。

Microsoft Windows 2000 Service Pack 4

http://www.microsoft.com/downloads/details.aspx?familyid=3DD3B530-7F43-4C18-8298-6E8797431A5D

Microsoft Windows XP Service Pack 1 および Microsoft Windows XP Service Pack 2

http://www.microsoft.com/downloads/details.aspx?familyid=EF402946-1C3B-47E9-9D51-77D890DF8725

Microsoft Windows Server 2003

http://www.microsoft.com/downloads/details.aspx?familyid=25469675-DF28-4889-8D13-25EFCD498388

Itanium システム向け Microsoft Windows Server 2003

http://www.microsoft.com/downloads/details.aspx?familyid=F0AEC064-34A3-4EE4-9F15-BE1E3DD02BC7

回避策
Microsoft は Print Spooler Service を無効にすることを推奨していますが、こうするとローカルおよびリモートの印刷も無効となってしまいます。

4-2 脆弱性 ID 100

○脆弱性情報

脆弱性名	MS03-043: Microsoft Windows Messenger Service Buffer Overrun Vulnerability
カテゴリ	バッファオーバフロー
危険度	非常に危険
リスクレベル	Remote Privileged
スキルレベル	Script
CVE	CVE-2003-0717

○脆弱性の内容

Microsoft Windows Messenger サービスは、クライアントコンピュータとサービスとの間で行き来するネット送信メッセージおよび Alerter サービスメッセージを送信します。このサービスは通常、管理者が使用して、スケジュール設定されたダウンタイムおよびネットワークステータスをユーザに伝えます。また、Windows および別のプログラムが使用して、ユーザに対する有益なメッセージが表示される可能性もあります。

Messenger Service は、割り当てられたバッファにメッセージを渡す前に、メッセージ長を正しく確認しません。この脆弱性により、攻撃者は、メッセージがバッファに渡された際オーバーフローが生じ、Messenger Service を機能不能にするという特別なメッセージを作成してしまいます。攻撃者が、バッファをオーバーフローさせ、ローカルシステム特権でコードを実行するメッセージを作成する可能性があります。
ローカルシステム特権で、攻撃者は、プログラムのインストール、ファイルの修正および削除、ならびに完全な特権がある新しいアカウントの作成ができてしまいます。

最新版が利用可能です。

長いネット送信メッセージが原因で発生する以外、この脆弱性に関する利用できる情報はありません。リモートの攻撃者は、試行錯誤して正しいメッセージ長を特定する可能性があります。

リモートの攻撃者は、Messenger Service を失敗させるまたは選択したコードを実行させる可能性があります。コードはローカルシステム特権で実行され、攻撃者はファイルの作成、修正、削除および実行、プログラムのインストール、ならびに完全な特権がある新しいアカウントの作成ができてしまいます。

解決策

適切なパッチをダウンロードし、この脆弱性を修正することをお勧めします。

ユーザは Messenger Service を無効にする、または NetBIOS ポート(137 から 139 まで)および UDP ブロードキャストパケットを遮断して、正しいパッチがインストールされるまで、攻撃を回避することができます。