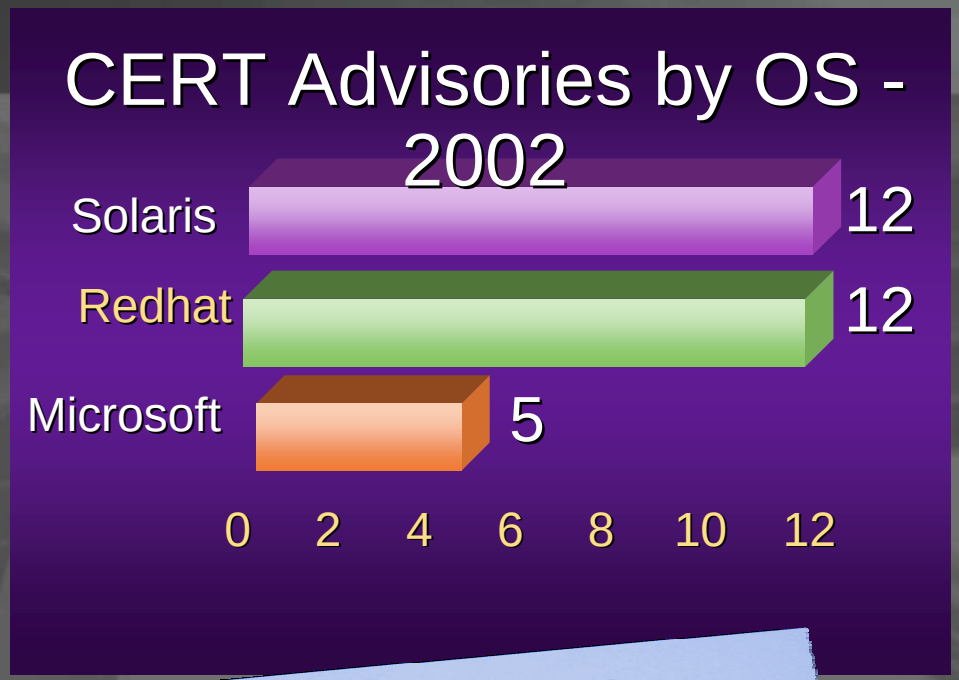
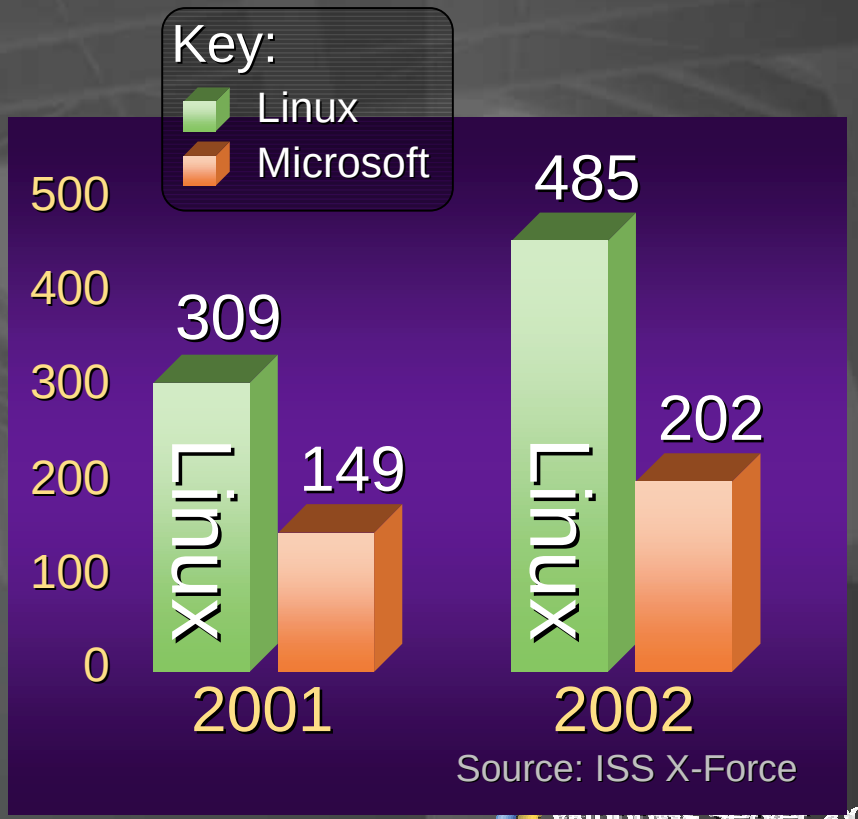
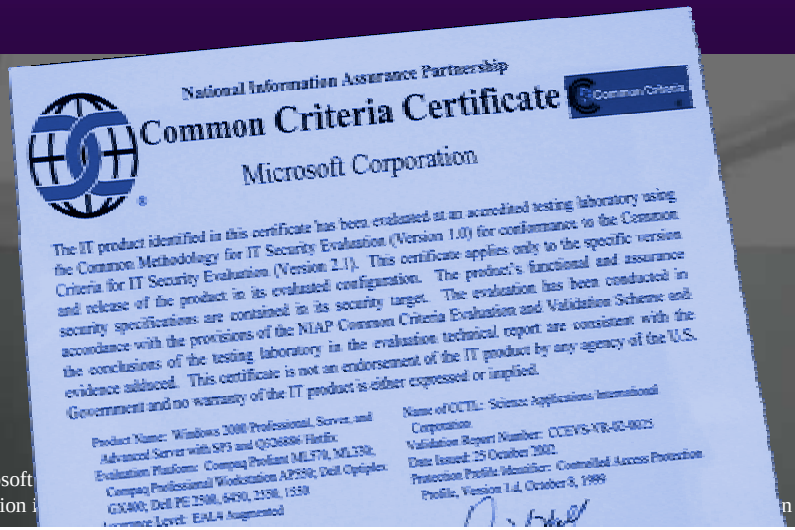
対岸の火事ではない



脆弱性の件数は議論の対象ではなくどう対応していくか業界全体の問題





National Information Assurance Partnership

Common Criteria Certificate

Microsoft Corporation

The IT product identified in this certificate has been evaluated at an accredited testing laboratory using the Common Methodology for IT Security Evaluation (Version 1.0) for conformance to the Common Criteria for IT Security Evaluation (Version 2.1). This certificate applies only to the specific version and release of the product in its evaluated configuration. The product's functional and assurance security specifications are contained in its security target. The evaluation has been conducted in accordance with the provisions of the NIAP Common Criteria Evaluation and Validation Scheme and the conclusions of the testing laboratory in the evaluation technical report are consistent with the evidence adduced. This certificate is not an endorsement of the IT product by any agency of the U.S. Government and no warranty of the IT product is either expressed or implied.

Product Name: Windows 2000 Professional, Server, and Advanced Server with SP3 and Q326886 Hotfix

Evaluation Platform: Compaq Proliant ML570, ML330; Compaq Professional Workstation AP550; Dell Optiplex GX400; Dell PE 2500, 6450, 2350, 1550

Assurance Level: EAL4 Augmented

Name of CCTL: Science Applications International Corporation

Validation Report Number: CCEVS-VR-02-0025

Date Issued: 25 October 2002

Protection Profile Identifier: Controlled Access Protection Profile, Version 1.d, October 8, 1999

しかし

7月2日	7月17日	7月26日	8月12日
脆弱性の発見と弊社への連絡、パッチの開発スタート	セキュリティ情報とパッチの公開、攻撃コード未確認	攻撃コードの公開	ワームの出現と拡散

脆弱性の連絡

- RPC/DDOM の脆弱性についての連絡を受ける
- 最高レベルのセキュリティ対応をスタート

セキュリティ情報

- MS03-026 をお客様に提供開始
- アナリスト、プレス、コミュニティ、パートナー、政府関係機関への連絡を継続的に実施

攻撃コード

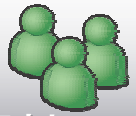
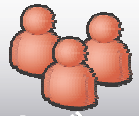
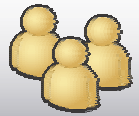
- X-focus が攻撃用コードを一般に公開
- カスタマへの最大限の告知を実施し、状況の理解を促進

インシデント

- Blaster ワームの出現と亜種、その他のウイルスが猛威を振るう SoBig, Swen

Blaster は、セキュリティ研究家やソフトウェアベンダー、そしてクラッカーの複雑に入り組んだ関係をあらわにした

悪用コード登場までのプロセス

セキュリティ調査組織	悪用コードの開発者	ワームの開発者
		
脆弱性の発見	パッチのリバース エンジニアリング & Webサイトへの悪用コードの公開	公開された悪用コードとワーム開発のためのツール キットを利用し、ワームをこぞって開発

マイクロソフトが行っていること

脆弱性を修正するために協力して作業	悪用コードの公開は不正な行為であるというコミュニティのコンセンサスの形成	法の執行当局との作業
責任をもって脆弱性情報を公開する	対話の継続	法廷上での作業における技術的支援

結果

無責任に脆弱性情報を公開してしまう調査機関の減少 製品品質の継続的改善	悪用コードの公開行為に対して業界のエキスパートが否定的発言をより多く行う	Blasterワームに関して、2件の検挙

セキュリティのさらなる向上
危機への対応策

- パッチの数が多い
- 悪用コード開発時間の短縮
- 悪用コードの攻撃手法はより洗練されたものに
- 現在のセキュリティ対策の方法では不十分

セキュリティはマイクロソフトの最重要項目
ただし、魔法のような解決策は存在しない
それでも、環境の変化は革新を必要としている

Windows Server 2003

お客様の声

「パッチの品質が低く、
適用プロセスに一貫性がない」

「マイクロソフト製品を企業で利用
する際のよい方法を知りたい」

「毎週新しいパッチが公開されたのでは、常に最新の状態に保つことは不可能」

「それでもなお、マイクロソフト
製品には多くの脆弱性がある
のでは」

マイクロソフトの
アクション アイテム

パッチおよびその適用
プロセスの改善

ガイダンスと
トレーニングの提供

パッチを適用しなくても、
脆弱性を軽減する

継続的な
製品品質の向上

Windows Server 2003

パッチおよびその適用プロセスの改善
新しいパッチ提供ポリシー

- パッチ無償提供サポート期間の延長 (2004年6月末)
  - Windows 2000 SP2 へのパッチの提供
  - Windows NT SP6a へのパッチの提供
- 緊急性を要さないセキュリティ パッチは月に一度のスケジュールでリリース
  - 月次でテストおよび展開ができるように事前に計画可能になる
  - まとめて適用できるように個々のパッチを一まとめのパッケージとして提供
  - セキュリティ ロールアップ パッケージにより、パッチ適用の柔軟性が向上

緊急性が要求される問題に対しては、今後も即時リリースは行う

Windows Server 2003

パッチおよびその適用プロセスの改善
パッチ自体の改善

お客様の要求	マイクロソフト対応
パッチ適用の複雑性の低減	2004年5月までに、Windows 2000以降のWindows、Office、SQLおよびExchangeのパッチ メカニズムを2種のインストーラに統合。全てのパッチが同一の挙動になる。 (SUS 2.0, MSI 3.0)
パッチ展開に関わるリスクの低減	現在：社内のテスト リソースの増員、リリース前のパッチをテストしていただくユーザー グループ 2004年5月までに、Windows, SQL, Exchange, Officeのパッチはロールバック機構を実装
パッチの容量の削減	現在: パッチ容量を35%またはそれ以上削減。 2004年5月までに、80%削減する。 (差分パッチ技術とMSI 3.0による機能改善)
ダウンタイムの削減	現在: Windows 2000以降でリブートを 10% 削減 2004年5月まで: Windows Server 2003 SP1で 30% 削減 次期Windows Serverで最高 70% 削減
全製品における パッチ適用の自動化	2003年11月: SMS 2003 (US) によりサポートされているすべてのマイクロソフトのプラットフォームおよびアプリケーション製品に対してパッチの適用を可能に 2004年末までに、マイクロソフト製品向けの全てのパッチの挙動は同一になり、かつ単一のロケーションより取得可能 (MSI 3.0 + SUS 2.0)

IT Pro向けセキュリティ ガイダンス

- セキュアな環境の運用管理にフォーカス
- 徹底的な対策のためのパターンと実践方法
- 企業のためのセキュリティチェックリスト – 信頼できるセキュリティ ガイダンスのための単一の情報源

patterns & practices

proven practices for predictable results

- 現在利用できるもの
  - 17 の実践ガイド
  - マイクロソフト社内でのセキュリティ対策情報ガイダンスとツール群
- 今年末から2004年を通じて
  - さらに多くのHow to情報および実践ガイドの提供
  - 共通タスクを自動化するツールとスクリプト群の提供

Windows Server 2003

クライアントのシールド技術の機能強化

内容

パッチが未適用でも、コンピュータを保護できるように機能強化
Windows XP SP2 (2004上半期)で提供し、その後も機能追加

効果

ネットワーク ベースの攻撃、添付ファイル形式のウィルスおよびバッファーオーバーランを抑止

キーとなる機能

- ネットワーク保護: ICF機能の強化と既定の設定での有効化
- 安全なe-mail環境: Outlook Express と IM機能での添付ファイルの無効化機能の強化
- 安全なブラウザ環境: 悪質なActiveXコントロールとスパイウェアのユーザーによる制御機能の改善
- メモリ保護: スタックのオーバーランを削減するコンパイラのチェックオプションの向上 (/GS スイッチ)

企業向けシールド技術の機能強化
企業システムの遮蔽

内容	企業のセキュリティ標準に適合するクライアントのみ接続を許可; Windows Server 2003 SP1 (2004上半期)で提供 し、その後も機能強化
効果	感染したコンピュータから企業資産を保護
キーとなる機能	• パッチの適用レベル、ウィルス対策ソフトウェアのシグニチャファイルの状態およびファイアウォール設定といった企業の特定のセキュリティ要件の強制機能 • 以下のケースにセキュリティ標準を検証 ➢ リモートクライアントからのVPN接続要求時 ➢ 不正または意図しないクライアントからの有線または無線での接続要求時