このパッチあてても大丈夫？

～セキュリティパッチの安全な普及のためにできること～

平成17年10月7日
株式会社ラック
三輪信雄

自己紹介

歴任、受賞など

Firewall MLオーナー、Firewall Defenders(FWD)会長
内閣官房情報セキュリティポリシーガイドラインWG委員
日本ネットワークセキュリティ協会(JNSA)理事　セキュリティポリシーWGリーダー
警察庁セキュリティビジネス調査WG委員、不正プログラム調査WG委員
会計検査院セキュリティセミナー講師、警察大学校講師
情報セキュリティ講座講師(早稲田大学、琉球大学)、総務省統一研修講師
情報ネットワーク法学会発起人
内閣官房情報セキュリティ基本問題委員会第一分科会、第二分科会委員他
セキュリティキャンプ2004,2005実行委員長、情報セキュリティ文化賞2005

現在

株式会社ラック 代表取締役社長
BUGTRAQ-JP モデレータ
データベース・セキュリティ・コンソーシアム事務局長

著書

「エクストラネット/イントラネット 実践!!セキュリティ対策」SRC出版
「セキュリティポリシーでネットビジネスに勝つ」NTT出版
「ネットワーク攻撃詳解」SRC出版、「ネットビジネスのセキュリティ入門」日経新聞社
「インターネット・セキュリティ教科書 」(共編)IDGジャパン

監訳

「セキュリティポリシーの作成と運用」ソフトバンクパブリッシング

監修

「ネットワークセキュリティとシステム開発」SRC出版
「不正アクセスの手法と防御」ソフトバンクパブリッシング

1．MS社との馴れ初め

- '99年6月英語版IISにリモートからバッファオーバフローによりコマンド実行可能な脆弱性が発見されBugtraqに「検証コード」と共に投稿される(MS99-019)。

- 「検証コード」は英語版にのみ効果があったが、日本語版での再現を「検証コードを作成」して再現の検証に成功し情報を公開した。その後日本語用パッチがMS社より提供される。

1．MS社との馴れ初め

'99年7月26日

- IISにリモートからDoS攻撃のできる脆弱性を発見しMS(USA)に報告。
- MSセキュリティチームとのやりとりのメールは数十通

'99年8月12日

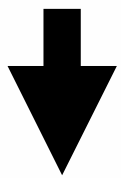
- パッチが公開される(MS99-029)
- パッチを適用するとハングアップすることがあることが判明、新しいパッチが出るまでインストールしないようにユーザに告知

'99年8月17日

- ハングアップする問題を解決したパッチが公開される

2. パッチのリリース期間が延びている？

- **脆弱性を発見するヒトとウィルスや攻撃ツールを作る人間は、いまのところ別人であることが多い**
- **紳士的に処理される仕組みが作られつつある**
- **脆弱性の存在への批判よりも、パッチの不具合に対する批判が非常に大きい**



脆弱性の発見から対策パッチ作成、公開までの期間が延びつつあるのでは？

3. パッチをあててください

- 日本ではパッチ適用率が高いらしい
- パッチをあてないと脆弱性を悪用した攻撃の対象となるかもしれない
- 脆弱性の発見者が秘密を守っているとは限らない
- 脆弱性の発見者はひとりではないかも
- パッチ適用は運用管理の仕事の一部

4. パッチをあてたくありません

① パッチをあてたら止まるかもしれない

- サーバの環境に依存するので予測不可能
- ハマった経験がある、聞いたことがある
- 調子が悪くなるなら、あてないほうがマシ
- 再起動したらハマった経験がある

② 「いつあてるか」が判断できない

- 緊急って言われても...
- つぎのメンテでまとめてやるから...

③ パッチをあてたくてもあてれません

- ドライバやアプリが対応していない

5．もし飛行機会社だったら？

- 欠陥がわかった部品を使っていたら、その事実だけで社会的に批判をあびる
- 重大な欠陥がある部品が見つかったら、運行を止めるか代替機を用意して部品を交換
- 想定範囲内での部品交換による運行続行の仕組みや環境の構築の責任がある
- 運行を止めて部品交換するかどうかは経営者の判断
- 人命より優先されるものはない

6．パッチを安全に利用するために

① パッチ適用のリスクは経営者が負う

- 大事なサーバをとめる判断
- パッチをあてないで運用を続けるリスク
- 公的基準が必要

② パッチによる不具合情報の積極的な共有

- 「勇気ある」ユーザグループによる事前テスト
- 「勇気ある」ユーザへのインセンティヴ
- MSによる積極的な情報収集、配信
- 不具合が生じなかった環境の情報公開
- 不具合が生じた環境の情報公開
- 巨大企業だからできるコトの提案と活用

6．パッチを安全に利用するために

③ 検証環境の構築は組織の責任

- 企業や顧客を守る重要なシステムにおける検証環境の構築と費用負担は、経営者の責任

④ ドライバやアプリケーションの対応

- 案1．パッチへの対応状況一覧の公開
- 案2．パッチへの未対応ベンダ一覧の公開
- 案3．「勇気あるユーザ」による検証情報共有
- 案4．パッチへの対応に積極的なベンダの表彰

6．パッチを安全に利用するために

⑤ パッチをあてなくても済む環境の構築

- サーバでのクライアントアプリの使用禁止
- ファイアウォールやパケットフィルタリングの設定による攻撃の無効化
- サーバとして不要なサービスの停止、削除
- パッチの必要性の理解
- パッチをあてなくても設定で逃げられることもある
- 脆弱性に対する深い技術的知識

7. MSさんへの要望

会場のみなさんの同意が得られるなら・・・

① パッチ不具合検証ユーザグループの構築

② パッチ不具合情報の積極的な情報公開

③ パッチ適用の必要性診断サイトの立上げ

④ ドライバやアプリのパッチ対応促進活動

⑤ 製品の品質向上への更なる努力

⑥ パッチの品質向上への更なる努力

メーカに責任を押し付けるだけでは解決しない問題です