

取扱体制の意義

- 公共の利益に資する脆弱性情報取扱の実現
- 情報の収集
 - － 脆弱性発見者と製品開発者の仲介
 - 未知の脆弱性をいらずに暴露されないようにする
 - 脆弱性発見者を保護する
- 情報の公表
 - － **製品開発者による情報の独占がもたらす弊害の回避**
 - 「闇改修」: 製品開発者が自力で自社製品に脆弱性を見つけて改修し、新バージョンをリリースしたが、旧バージョンに脆弱性が存在する事実を公表しないという事態
 - 不明瞭な告知: 製品開発者が、脆弱性の修正を告知する際に、その脆弱性のリスクを過小評価、矮小化した表現をする事態
 - － 製品開発者は必ずしも公共の利益のために行動しない

5

対策情報の「公表マニュアル」

- 「ソフトウェア製品開発者による脆弱性対策情報の公表マニュアル」を提供, 2007年6月
 - － 情報システム等の脆弱性情報の取扱に関する研究会編
 - － 目的: 不慣れな製品開発者に開眼を促す
 - 意図的に隠蔽、矮小化する製品開発者に対する強制力はない
 - － 内容
 - 脆弱性対策について利用者が必要としている情報
 - 脆弱性対策情報の公表項目と公表例
 - 望ましい公表の例、望ましくない公表の例、望ましくない理由
- 類似の話: 「リコール社告のJIS化」
 - － 「消費者が望むJIS規格」, 主婦連合会

6

「JVN」での公表（例）

公開日: 2007/12/11 最終更新日: 2007/12/11

JVN#90712589
複数のサイボウズ製品におけるクロスサイトスクリプティングの脆弱性

概要
複数のサイボウズ製品には、クロスサイトスクリプティングの脆弱性が存在します。

影響を受けるシステム

- サイボウズ Office 6.6 (1.3) およびそれ以前
- サイボウズ ガルーン 1.5 (4.1)
- サイボウズ ガルーン ワークフロー 1.0 (1.1) およびそれ以前
- サイボウズ ガルーン ファイル管理サーバー 1.0 (0.7) およびそれ以前
- サイボウズ ガルーン 掲示板サーバー 1.0 (0.7) およびそれ以前
- サイボウズ ガルーン 施設予約サーバー 1.0 (0.7) およびそれ以前
- サイボウズ ドットセルス 1.0 およびそれ以前

詳細情報
複数のサイボウズ製品には、クロスサイトスクリプティングの脆弱性が存在します。なお、本脆弱性はJVN#50342989とは異なる問題です。

想定される影響
ユーザのウェブブラウザ上で任意のスクリプトを実行される可能性があります。

7

一太郎にZero-day攻撃

- 一太郎zero-day攻撃の発生を伝える報道（第一報）「INTERNET Watch」より
 - － 2006年8月17日: 「一太郎」の未知の脆弱性を悪用するウイルスが出現、**シマンテックが警告**
 - － 2006年9月28日: **シマンテック**、「一太郎」の未知の脆弱性を狙うトロイの木馬を**再び警告**
 - － 2007年4月9日: 「一太郎」の未知の脆弱性を狙ったウイルス、**Symantecが警告**
 - － 2007年8月3日: 「一太郎」の未知の脆弱性を狙うトロイの木馬、**シマンテックが警告**
 - － 2007年12月14日: 一太郎の脆弱性を狙う新たな攻撃、集中的に狙われていると**Symantecが警告**

8

何が起きている？

- 政府機関を狙ったtargeted attackが継続して起きている？
 - － 公表されていないので不明
 - 意識的に公表を控えているのか、単に実態把握ができていないだけなのか(私は知らない)
 - － 極めて少数の事例報告(従来型のウイルスと違って)
 - － 一太郎と言えば.....どこで使われている？
- 「警察を標的にしたスパイ型フィッシング・メールが増加」— 警察庁 坂明氏, 日経IT Pro, 2006年5月29日
 - － 「警察や防衛庁を標的とする, 特定の対象を狙った偽装メール, いわゆるスパイ型フィッシング・メールが増加, かつきわめて精巧になってきている」— 警察庁 生活安全局 情報技術犯罪 対策課(サイバー犯罪対策課) 課長 坂明氏は5月26日から28日にかけて開催された「第10回コンピュータ犯罪に関する白浜シンポジウム」の講演で, 警察庁を標的とする攻撃が増加していることを明らかにした.
 - 「フィッシング」というのはちょっと違うと思うが

9

発覚経緯の謎

- なぜいつも Symantec から？
 - － 詳細はいつも英文blogで明らかにされる(ウイルス対応情報とは別に)
 - － 日本のメディアはそれを情報源として報道
- 誰かがウイルス検体を Symantec に提供？
 - － 憶測: どこかの官庁の情報システム管理者 → [検体提供] → (株)シマンテック → [丸投げ] → Symantec Corporation → [分析] → Symantec Security Response Weblog
- 情報源は公表されない
- ウイルス情報は、他の提携アンチウイルスベンダ間で共有されているのだろうが.....
- 製品開発者であるジャストシステムへはどんな経路で、どんな情報が伝えられたのだろう？

10

告示は及ばない？

- 当該脆弱性の発見者は Symantec
- Symantecから公表された2006年8月、9月、2007年4月、8月、12月の5件のzero-dayの脆弱性は、いずれもJVN (VN-JP) での公表に載っていない
 - － Symantecは「発見者基準」に従った届出をしていないと推察
- 外国企業に経済産業省告示は及ばない？
 - － そもそも「推奨」なので義務ではないにしても
- 日本法人はどうなの？ 日本人従業員はどうなの？

11

V. 対象がソフトウェア製品である場合の脆弱性関連情報取扱基準

- 一. 発見者が製品開発者ではない、又は、発見者が製品開発者であり発見若しくは取得した脆弱性関連情報の影響範囲が自社のソフトウェア製品に限らない場合
 - － 1. 発見者基準
 - (1) 発見者(自ら開発等を行ったソフトウェア製品に影響範囲が限られると認められる脆弱性関連情報を発見又は取得した製品開発者を除く。)は、発見又は取得した脆弱性関連情報を経済産業大臣が別に指定する受付機関に届け出ること。ただし、当該製品開発者に対し同じ内容を届け出ることを妨げない。
- 二. 発見者が製品開発者であり、発見又は取得した脆弱性関連情報の影響範囲が自社のソフトウェア製品に限られる場合
 - － (1) 製品開発者は、自ら開発等を行ったソフトウェア製品に影響が限られると認められる脆弱性関連情報を発見又は取得した場合、対策方法を作成し、当該脆弱性関連情報及び対策方法を受付機関及び調整機関に通知すること。

12

製品開発者による届出（通知）

- ジャストシステムは脆弱性情報を通知しているか？（私は知らない）
 - － アンチウイルスベンダから情報提供を受けて脆弱性を修正するとき、当該製品開発者も「脆弱性発見者」に該当するのでは？
- 製品開発者自身からの届出による取り扱い事例
 - － JVN#35677737: ソニー製指紋認証機能つき「ポケットビット」付属ソフトウェアにおける脆弱性

| | | | | |
|------------|--------------------------------------|--|-----------|-----|
| 18 (*2) | ソニー製指紋認証機能つき「ポケットビット」付属ソフトウェアにおける脆弱性 | ソニー製 USB メモリ「ポケットビット」のうち指紋認証機能付きの製品に付属するソフトには、特定のフォルダを不可視にする問題があります。このため、不可視化されたフォルダを、第三者により意図しない用途で利用される可能性があります。 | 2007年9月7日 | 2.6 |
|------------|--------------------------------------|--|-----------|-----|

- (*1): オープンソースソフトウェア製品の脆弱性
(*2): 製品開発者自身から届出られた自社製品の脆弱性
(*3): 複数開発者・製品に影響がある脆弱性
(*4): 組み込みソフトウェア製品の脆弱性

13

Zero-day攻撃発生中なのに届出必要？

- たしかに、パッチ提供の目的では不必要
 - － 通常は、「攻撃に悪用されないよう、パッチ公開まで脆弱性情報を管理する」ということが、脆弱性情報取扱の目的
 - － この点は、zero-day攻撃発生時には必要とされない
 - 悠長なことをやっていないで直ちに警告を発することが正義とも言える
- しかし、脆弱性情報取扱の目的はそれだけではない

14

何が問題なの？

- 「パッチは出るんだからそれでいい」という話ではない
- 実害事例
 - － 一連の一太郎の脆弱性は、危険度が過小評価されている
 - 「出所の不明な一太郎文書ファイルを開かなければ回避できる」と誤った情報が流通している
 - － 実際は、「悪意あるWebサイトを閲覧しただけで被害」が正しい
 - － Symantecのblogにそのような（誤った脅威評価に基づく）記述
 - 日本のメディアはそれをそのまま報道
 - － 他に公式情報がないのでそうせざるを得ない
 - － ジャストシステムもそのように発表
 - 指摘を受けて若干修正した（2007年10月）が、2007年12月にも誤解を招く表現のまま発表
- 原因構造
 - － アンチウイルスベンダにとって脆弱性分析はビジネス上、必要でない
 - － 製品開発者は必ずしも公共の利益のために行動しない

15

問題点

- 公共利益の観点からの脆弱性分析ができない
 - － 危険度の正しい評価が必要
 - 製品開発者が自らそれを行うとは限らない（しないところが多い）
 - アンチウイルスベンダはそのことに関心がない
 - － 脆弱性分析に必要な情報が得られない
 - ウイルス検体はクロードに管理される
 - 攻撃パターンがtargeted attackに移行しているため入手が困難化
- 民間での話だったら、まあ、しかたないことかもしれない

16

政府における問題

- 今起きていることの仮定(推定)
 - どこかの官庁がtargeted attackに遭っている
 - 情報システム管理者が独断でアンチウイルスベンダに検体を提供して、それだけで対応を済ませている
 - もしくは、組織の決定事項としてそのような手順を実施している?
- とすれば、その問題点は
 - 日本国政府が攻撃に遭っているのに、**正しい対策情報**が流布されず、その原因が外国企業による情報の独占によるもの、そしてその元となる情報の提供者が政府部内の人、しかもそれは悪気なくやっている——という構図
- これはいかにも情けない話
 - しかし、現状では他に行動のとりようがない
 - ウイルス発見者は「脆弱性発見者」ではない(必ずしも)

17

提案

- 公共利益の視点からマルウェアの解析を担う組織が必要
 - 解析をアンチウイルスベンダに外注するのもよい
 - 解析が外国で行われるのだとしてもそれ自体が問題と言っているのではない
 - 目的が異なる
 - 通常のアンチウイルスベンダの目的 → パターンファイルを作成すること、blogでちょっと話題を提供すること「zero-day攻撃発生!!」
 - 公共の発注に基づく目的 → 脆弱性の存在とその影響範囲の分析、またはそれに必要な詳細情報の提供
- 脆弱性情報取扱との連携
 - マルウェア解析からの未知の脆弱性発見 → 脆弱性情報取扱
- IPAの既存の「ウイルス届出」窓口
 - 平成7年通商産業省告示第429号「コンピュータウイルス対策基準」
 - 目的が異なる: 「ウイルス被害の拡大及び再発を防止するため」
 - 形骸化していて、誰も届けていないのでは?
 - ウイルス届出数の計数とその公表しか役割を果たしていない

18

おわり

19

おまけ

- 脆弱性情報取扱制度の現時点の課題
 - 危険度の分析が十分に行われていない(じつは)
 - JVN公表時、製品開発者の公表した情報しか公表しない
 - 発見者(私)が指摘した危険性について、製品開発者が公表しない場合、JVNこそが正しい情報を提供する限られた公式な場なのに.....
 - もちろん、発見者の言うことを鵜呑みにして公表するわけにはいかない
 - 自力で危険度を分析する能力と、公表に向けての覚悟が必要

20

講演後追記

21

マルウェア解析の目的

- 「マルウェア解析」とは?
 - (a) そのマルウェアがどんな挙動をするか(攻撃の内容)
 - (b) そのマルウェアはどんな脆弱性を突いているか、あるいは突いていないか(攻撃可能化の手段)
- 提案で「マルウェアの解析を担う組織が必要」と言ったのは、
 - マルウェアの挙動(a)を解析する話ではない
 - 目的は未知の脆弱性の発見(b)とその報告
 - 「不特定多数の者に対して引き起こされる被害を予防」する観点からは、重要なのは脆弱性の情報であって、個々の攻撃内容の情報ではない
- もっとも、
 - 政府機関に対する攻撃については、攻撃内容を把握する必要性から、(a)の分析を国が行うべきという考え方もあるだろうが、
 - 私の提案はそれとは**独立した別の話題**
 - マルウェアの挙動解析(a)はアンチウイルスベンダーにおいてビジネスとして成立しているのに対し、脆弱性分析(b)はそうっていない
 - (a)の解析中に(b)の解析も同時に行えることから、アンチウイルスベンダーへの外注が合理的ではないかという話

22