Internet Week 2008

xSPにおける脆弱性対応について

IIJ Internet Initiative Japan

2008/11/27

株式会社インターネットイニシアティブ
サービス事業統括本部 セキュリティ情報統括部
IIJ-SECT
斎藤衛

Ongoing Innovation

xSPって？

- **今日の議論では**ISP、ASP、MSP**などを考える。**
  - Microsoft Update **は考えない。**
  - SIer**や**Stand Alone**な人は考えない。**
- xSP**の特徴**
  - **事業者の数が多い(届出通信事業者で約**14,000**社)**
  - **数十～数十万台くらいの設備を扱っている。**
  - **顧客にサービスを提供している。顧客の中に**xSP**もいるが、同じに扱う(今日はインフラ魂の議論はしない)。**

xSPにおける脆弱性対応って？

- やること
  - 情報入手して
  - 関係あるかどうか判断
  - 検証する (影響範囲とか深刻さを検討)
  - ワークアラウンドの有無を調査
  - 対策 (ワークアラウンドの設定、バージョンアップ)
  - 効果測定(攻撃の有無の確認も含む)
- 対応の組織はさまざま
- 全部できているのは理想的なxSPか？

xSPにおける脆弱性対応の優先順位

- 脆弱性の深刻さの評価
  - サービスの停止
  - Remote exploitableなもの
  - その他

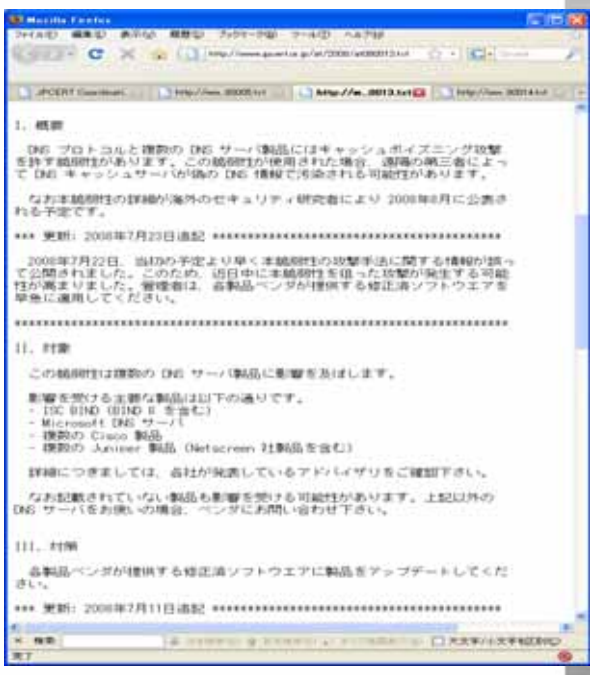
- 対応検討時の優先順位
  - 対象装置でのワークアラウンド
  - 構成的対応
    (サーバの脆弱性に対してルータでフィルタ、など)
    :
  - ソフトウェア/ファームウェアのバージョンアップ

脆弱性対応情報を受け取る

バトンをちゃんと渡してもらわないと。。。

適切な情報提供を

- 複数の DNS サーバ製品におけるキャッシュポイズニングの脆弱性 (JPCERT/CC Alert 2008-07-24)
  - 誰に向けた注意喚起なのか？
  - 影響範囲の記述は？
  - 検証方法の記述は？
- 副作用
  - 顧客からの問い合わせの増加
- 違う人が書いてます？
  - 対象が明確な情報を記載した注意喚起もある (たとえばSQLインジェクションの注意喚起)
- NHKの報道



1. 概要

DNS プロトコルと複数の DNS サーバ製品にはキャッシュポイズニング攻撃を許す脆弱性があります。この脆弱性が使用された場合、通常の第三者によって DNS キャッシュサーバが偽の DNS 情報で汚染される可能性があります。

なお本脆弱性の詳細が海外のセキュリティ研究者により 2008年8月に公表される予定です。

*** 更新: 2008年7月23日追記 ***

2008年7月22日、当初の予定より早く本脆弱性の攻撃手法に関する情報が誤って公開されました。このため、近日中に本脆弱性を狙った攻撃が発生する可能性が高まりました。管理者は、各製品ベンダが提供する修正済ソフトウエアを早急に適用してください。

II. 対象

この脆弱性は複数の DNS サーバ製品に影響を及ぼします。

影響を受ける主要な製品は以下の通りです。
- ISC BIND (BIND 8 を含む)
- Microsoft DNS サーバ
- 複数の Cisco 製品
- 複数の Juniper 製品 (Netscreen 社製品を含む)

詳細につきましては、各社が発表しているアドバイザリをご確認下さい。

なお記載されていない製品も影響を受ける可能性があります。上記以外の DNS サーバをお使いの場合、ベンダにお問い合わせ下さい。

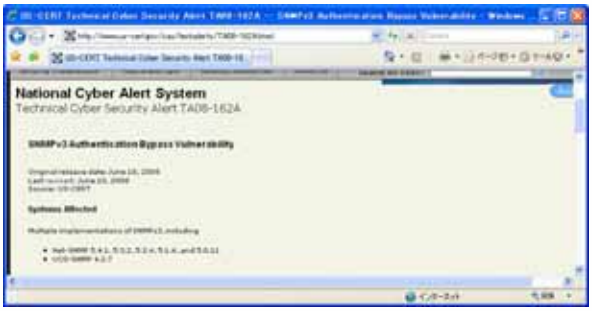
III. 対策

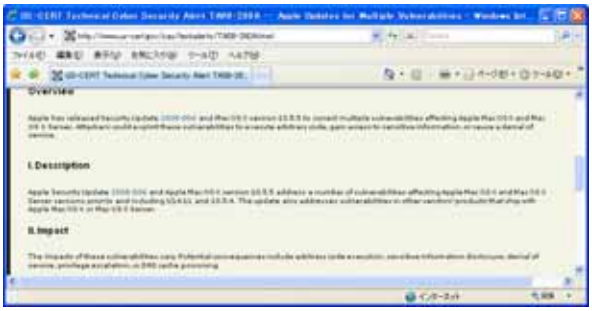
各製品ベンダが提供する修正済ソフトウエアに製品をアップデートしてください。

*** 更新: 2008年7月11日追記 ***

適切な情報提供を（2）

- 脅威評価できてます？
  - SNMP v3の US-CERT Technical Cyber Security Alert (TA-08-162A)
  - 誰が使っている？
- 何を伝えようとしています？
  - Apple MAC OS X の US-CERT Technical Cyber Security Alert (TA08-260A)
  - 怖いことだけ書いてある

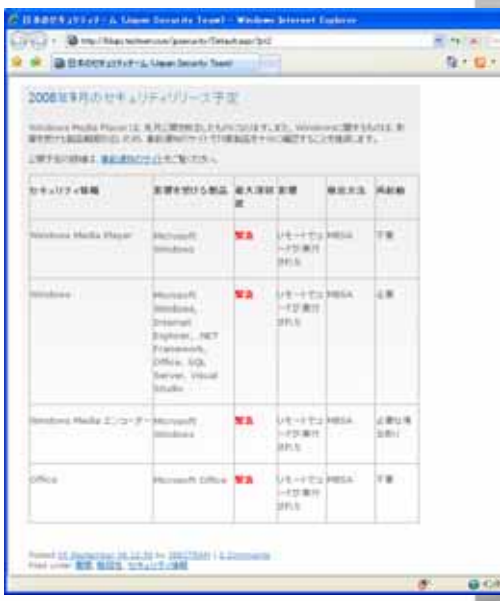




Internet Initiative Japan Inc.

定例パッチの光と影

- 代表的な定例リリース
  - Microsoft(月に1回)
  - Cisco(年に2回)
  - Oracle(年4回)
- 光の部分
  - 定例リリースは優先情報提供の一種である
  - ソフトウェア・ファームウェアアップデートのタイミングを集約できる
  - 作業・人員計画が立てられる（かもしれない）
- 影の部分
  - 一斉リリースでは作業量見積もりが困難
  - リリース日はむちゃくちゃ忙しくなる、こともある
- Microsoft の事前通知は少し良い
  - 対象が明確になる



DNS Cache Poisoning (Kaminsky 2008) 対応からの反省

- タイムテーブル
  - 07/09 注意喚起、パッチ
  - 07/22 事前リーク
  - 08/07 BlackHatでの発表
- 事業者側の反省点
  - NAT箱対応はまだ終わっていない（かも）
  - スケジューリングはお尻から

どうしたいか

- 注意喚起について
  - 誰あての注意喚起なのかを明確にしてください
- xSP事業者向け情報提供について
  - 優先情報提供の体系構築を
    - 一般公開前にxSP事業者への情報提供を検討しませんか
    - 機密保持契約結べる範囲でかまいません
  - 対応作業の計画が立てられる内容の情報発信を
    - 脆弱性情報ハンドリングには「公表日一致の原則」があるそうですが、たとえば、脆弱性の存在の公開、パッチの公開、詳細の公開という順番でも問題ないのでは？(DNS Cache Poisoning, Intel , Sockstress ,SSH,…)

IIJ Internet Initiative Japan

ご清聴ありがとうございました

Ongoing Innovation