Windowsにおける暗号強度の強化について

1024 bit未満のRSA証明書のブロック　2012/8/14　(更新 2012/9/3)

- **1024ビット未満のRSA暗号 をブロックする更新プログラムを公開(Windows 8はRTMで対応済み)**
  - **暗号の危殆化に伴う証明書の偽装が確認されたため（証明書に対するコリジョン攻撃の成功）**
- **10月にはMicrosoft Updateで提供を開始するため、それまでに影響を確認する必要があります**

証明書の利用例

- 商用認証局が発行する証明書
  - サーバー証明書、クライアント証明書など
  - コード署名、S/MIMEなど
- 自社認証局で発行した証明書
  - 通信/VPN向け：IPsec, SSL/TLS, 802.1x認証
  - クライアント証明書、スマートカードなど
  - EFSなどの暗号処理、コード署名など

主にクライアントに対する影響

- Webアクセス（SSLによるアクセス）
  - 特定のサイトがWindowsから利用できなくなる可能性がある
  - 携帯電話向けとＰＣ向けを共用しているサイトで、512bit RSAの利用が懸念されています
- 認証関係
  - ターミナルサーバー、スマートカード、無線LAN、VPN接続
- ソフトウェア
  - 暗号を利用するソフトウェア、
  - コード署名(アプリケーション, ActiveX, スクリプト)

主にサーバーに対する影響

- メールサーバー（POP over SSLなど）、VPN装置、様々な認証
- SSLを利用して接続する装置（例えば、電源管理装置など）
- Webアプリケーション、ミドルウェアなどのコード署名

確認された影響

- **携帯電話向けを兼ねたWebサイトがRSA-512を使用していた**
- **ソフトウェアのコード署名がRSA-512を使用していた**
- **全社展開のクライアント証明書がRSA-512を使用していた**

なぜ対策が必要なのか

- **信頼の基盤（Trusted Anchor)の喪失を防ぐ**
  - 証明書は、認証や暗号といったシステムや情報を保護するための基盤となる技術で、証明書の偽造が可能になる（危殆化）と信頼の基盤が崩れ、対処の難しい多くの問題に直面します
  - 信頼基盤の喪失を避けるため、コンピューターの性能の向上に合わせて、安全性の高い暗号に更新していく必要があります

影響の確認手順

- **証明書の確認**
  - 商用認証局から購入しているRSA証明書の鍵長を確認します（現在、サーバー証明書は2048bitが標準です）
  - 自社認証局で発行しているRSA証明書の鍵長を確認します
- **実機による検証**
  更新プログラムを適用し、ブロックされる証明書が存在しないか、実地調査を行います
- **該当する証明書の対応**
  - 商用認証局が発行する証明書は、商用認証局にお問い合わせください
  - 自社で発行している場合は、暗号の鍵長を1024ビット以上（できれば2048ビット）に設定し、再発行を行ってください

RSA1024ビット未満の証明書を使い続けるには

- **更新プログラムを適用する**
  - 該当する証明書の存在を確認するためにも、更新プログラムを適用するようにしてくだい
- **最低暗号鍵長を設定する**
  - 鍵長を必要な長さに設定し、展開してください
- **該当する証明書を把握する**
  - 上記検証方法で、該当する証明書を把握し、できるだけ早く安全な証明書に切り替えてください

暗号強度強化の背景と参考資料

(更新 2012/9/3)

Flameの偽装証明書によるWindows Updateを使った攻撃

マルウエア(Flame)が偽装したマイクロソフトの証明書でコード署名

- Windows Updateを使ってイントラネット内で拡散
- MD5ハッシュに対するコリジョン攻撃に成功（暗号の危殆化）
- 同じ暗号強度の証明書は偽造可能な状況と推定されている

マイクロソフトの対応	
該当する証明書を失効処理（無効化）	6/3 SA 2718704
新しい公開鍵証明書を配布	6/6
Windows Update エージェントの更新	6/8 KB949104・KB2720211
失効処理専用のプログラムを追加	6/12 月例更新KB2677070
弱い暗号を利用している証明書を更新	7/11 月例　SA 2728973
1024ビット未満のRSAをブロック	8/14　KB2661254
上記　KB2661254を自動配信	10月の月例を予定

MD5と1024ビット未満のRSAの危殆化（解読可能性）について

- 2005年にはNIST SP 800-57により2011年までに利用中止を勧告
- このため、認証局では2048bitの証明書を推奨している
  NIST Special Publication 800-57 (March, 2007)　第２版
  Recommendation for Key　Management – Part 1: General
  http://csrc.nist.gov/publications/nistpubs/800-57/sp800-57-Part1-revised2_Mar08-2007.pdf

Flameと証明書についての参考資料

日本マイクロソフト

2012 年 6 月のセキュリティ情報 (月例) – MS12-036 ～ MS12-042
http://blogs.technet.com/b/jpsecurity/archive/2012/06/13/3503546.aspx
セキュリティ アドバイザリ 2718704: Flame の攻撃と WU の強化
http://blogs.technet.com/b/jpsecurity/archive/2012/06/11/3503098.aspx

SRD　BLOG

Microsoft certification authority signing certificates added to the Untrusted Certificate Store
http://blogs.technet.com/b/srd/archive/2012/06/03/microsoft-certification-authority-signing-certificates-added-to-the-untrusted-certificate-store.aspx
Flame malware collision attack explained
http://blogs.technet.com/b/srd/archive/2012/06/06/more-information-about-the-digital-certificates-used-to-sign-the-flame-malware.aspx

影響の確認手順

- **証明書の確認**
  - 1024 ビット未満の暗号キーをブロックする更新プログラム (KB2661254) を 8/14 に公開 - その 2
  - http://blogs.technet.com/b/jpsecurity/archive/2012/08/10/3513621.aspx
- **実機による検証（イベントログ）**
  - 1024 ビット未満の暗号キーをブロックする更新プログラム (KB2661254) を 8/14 に公開
  - http://blogs.technet.com/b/jpsecurity/archive/2012/07/30/3511493.aspx
- **該当する証明書の収集**
  - 1024 ビット未満の暗号キーをブロックする更新プログラム (KB2661254) を 8/14 に公開 - その 3
  - http://blogs.technet.com/b/jpsecurity/archive/2012/08/14/3514260.aspx
- **該当する証明書の対応**
  - 商用認証局から購入している証明書については、認証局にお問い合わせください
  - 自社で発行している場合は、暗号の鍵長を1024ビット以上（出来れば2048ビット）に設定し、再発行を行ってください

ブロックされる証明書を有効にする

- **Certutil**コマンドを使い、ブロックする鍵長を変更できます
- ただし、暗号の安全性が低い状態のままであるため、できるだけ早く安全証明書に更新し、設定を戻してください
  - 例：　**Certutil** -setreg chain¥minRSAPubKeyBitLength 512 (Vista以降)
  - レジストリでも設定可能です。詳しくは、以下のBLOGをご参照ください
- 1024 ビット未満の暗号キーをブロックする更新プログラム (KB2661254) を 8/14 に公開
- http://blogs.technet.com/b/jpsecurity/archive/2012/07/30/3511493.aspx

MSRC　BLOG

Microsoft releases Security Advisory 2718704
http://blogs.technet.com/b/msrc/archive/2012/06/03/microsoft-releases-security-advisory-2718704.aspx
Security Advisory 2718704: Update to Phased Mitigation Strategy
http://blogs.technet.com/b/msrc/archive/2012/06/04/security-advisory-2718704-update-to-phased-mitigation-strategy.aspx
Security Advisory 2718704: Collision attack details, WU update rollout
http://blogs.technet.com/b/msrc/archive/2012/06/06/security-advisory-2718704-collision-attack-details-wu-update-rollout.aspx