— AUS（アルテミス・ユーザ・サポート）便り 2016/10/17号 —
http://www.artemis-jp.com

ここで紹介するニュースは、ほとんどの場合、日頃からOS・アプリケーション・アンチウイルスのデータベース等を常に最新の状態に保つこと、併せて、UTM導入等によるネットワーク全体の防御を行うことで対策できます。

●Windows7までにローカルからのDoS攻撃の脆弱性、推奨対策は「8.1/10へのアップグレード」

http://www.itmedia.co.jp/enterprise/articles/1610/07/news095.html
https://jvn.jp/jp/JVN20786316/index.html

このニュースをザックリ言うと・・・

- 10月7日（日本時間）、IPAおよびJPCERT/CCより、Windows Vista/7にサービス拒否（DoS）攻撃につながり得る脆弱性が存在すると発表されました。

- 脆弱性はWindowsの暗号化APIである「Cryptography API: Next Generation (CNG)」に存在し、細工した鍵データを処理させることにより、PCを異常終了させられる可能性があるとされています（ただし、リモートから脆弱性を突くことは困難で、せいぜいローカルからの攻撃が可能な程度とみられ、危険度は高くない模様です）。

- 日本マイクロソフトによれば、Windows8.1/10に含まれるCNGには脆弱性はないとのことで、対策として、これらのWindowsへのアップグレードを推奨しており、10月12日に公開された月例のセキュリティパッチにもこの脆弱性への対策は含まれていない模様です。

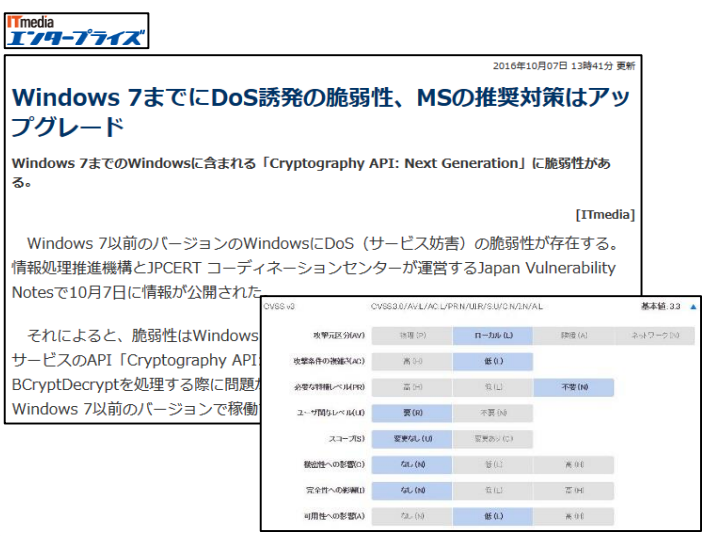
AUS便りからの所感等

- Windows7のセキュリティパッチは2020年1月までリリース予定ですが、厳密には「延長サポート」期間に入っており、「メインストリームサポート」は2015年1月に終了しています（Vistaについては2017年4月に延長サポートが終了予定です）。

- Windows7以前についてメインストリームサポートが終了したことにより、既に新しいハードウェアへの対応等は行われなくなっており、必ずしも重大ではないとは言え、全ての脆弱性にセキュリティパッチがリリースされるとは限らなくなってきているようです。

- 一方で、最新のWindowsであるWindows10について、最初の正式版リリースから1年、先日いわゆる「Anniversary Update」がリリースされたものの、環境によっては必ずしも動作が安定しないという評判もちらほら聞かれます。

- あと3年猶予があるとは言え、Windows10への移行は避けては通れない道であり、複数のPCへのWindows10の導入にあたっては、可能な限り十分な試験を行い、統一された環境へ導入することが鉄則と言えます。


ITmedia エンタープライズ

2016年10月07日 13時41分 更新

Windows 7までにDoS誘発の脆弱性、MSの推奨対策はアップグレード

Windows 7までのWindowsに含まれる「Cryptography API: Next Generation」に脆弱性がある。

[ITmedia]

Windows 7以前のバージョンのWindowsにDoS（サービス妨害）の脆弱性が存在する。情報処理推進機構とJPCERT コーディネーションセンターが運営するJapan Vulnerability Notesで10月7日に情報が公開された。

それによると、脆弱性はWindows サービスのAPI「Cryptography API BCryptDecryptを処理する際に問題 Windows 7以前のバージョンで稼働

CVSS v3　CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:N/I:N/A:L　基本値: 3.3

攻撃元区分(AV)	物理 (P)	ローカル (L)	隣接 (A)	ネットワーク (N)
攻撃条件の複雑さ(AC)	高 (H)	低 (L)		
必要な特権レベル(PR)	高 (H)	低 (L)	不要 (N)	
ユーザ関与レベル(UI)	要 (R)	不要 (N)		
スコープ(S)	変更なし (U)	変更あり (C)		
機密性への影響(C)	なし (N)	低 (L)	高 (H)	
完全性への影響(I)	なし (N)	低 (L)	高 (H)	
可用性への影響(A)	なし (N)	低 (L)	高 (H)	


公開日：2016/10/07　最終更新日：2016/10/07

JVN#20786316
Cryptography API: Next Generation (CNG) におけるサービス運用妨害 (DoS) の脆弱性

概要
Cryptography API: Next Generation (CNG) には、サービス運用妨害 (DoS) の脆弱性が存在します。

影響を受けるシステム
- Windows 7 以前の Windows に含まれる Cryptography API: Next Generation (CNG)

開発者によると、Windows 8 以降に含まれる CNG は本脆弱性の影響を受けないとのことです。

詳細情報
Cryptography API: Next Generation (CNG) には、BCryptDecrypt の処理に起因するサービス運用妨害 (DoS) の脆弱性が存在します。

想定される影響
細工された鍵データを Cryptography API: Next Generation (CNG) で処理することで、当該製品を異常終了させられる可能性があります。

対策方法
アップグレードする
開発者によると、Windows 8 以降に含まれる Cryptography API: Next Generation (CNG) は本脆弱性の影響を受けないとのことです。
OS を Windows 8.1 以降にアップグレードしてください。

●国会図書館検索でスマホ現在地漏えいの恐れ

http://www.yomiuri.co.jp/science/goshinjyutsu/20161005-OYT8T50089.html

このニュースをザックリ言うと･･･

- 10月5日（日本時間）、情報セキュリティに詳しいジャーナリストの三上洋氏らにより、国立国会図書館の検索機能「国会図書館サーチ」をスマートフォンで使用した場合に、ユーザの現在位置が漏えいする恐れがあると警告されています。

- 記事によれば、国会図書館サーチによる検索結果のURLには末尾にスマートフォンの位置情報による「?lat=35.xxxxx&lng=139.xxxxx」という文字列が付加されるとのことで、このURLをSNS等にそのまま貼りつけることにより、URLを見た人からは投稿者が検索時にどこにいたかが分かってしまうとされています。

- URLが付加されているのは国会図書館サーチの「近くの図書館を表示する」機能に関連したものとされていますが、記事の掲載後、国会図書館より、当該機能を無効化しURLに位置情報を含めないよう修正を行った旨が発表されています。

AUS便りからの所感等

- 特に子供など情報リテラシーが高くないユーザがスマホアプリ実行中のスクリーンショットを投稿し、そこから位置情報が推測できてしまうというケースはよく見られますが、一方で、誰かがうっかり公開した位置情報を悪意のある者が入手し、何らかの嫌がらせに悪用することも珍しくありません。

- 記事では、「図書館の利用履歴は重要なプライバシーである」ことを挙げ、位置情報が露呈する仕様であることを問題視しており、自衛策として、スマホのウェブサイトで「位置情報を利用します。よろしいですか？」と表示された場合は安易に了承しないことを挙げています。

YOMIURI ONLINE

<写真1>国会図書館サーチでiPhone（iOS 9. 3. 5）から蔵書検索した結果のページ。URLに緯度と経度が含まれている

- 人気のスマホアプリでも、その動作には不要なはずのスマホ上の情報へのアクセスを要求するものもまだ存在しますので、可能な限りアプリにそういったアクセス許可を渡さないよう慎重な利用を心がけるべきです。

●関西学院大学、個人情報1466人分流出･･･フィッシングサイトに誘導

https://cybersecurity-jp.com/news/12726

このニュースをザックリ言うと･･･

- 10月7日（日本時間）、関西学院大学より、同大学院理工学研究科および2006～2013年在籍の博士前期課程の学生、計1466人分の個人情報（氏名・生年月日・住所・電話番号等）が流出したと発表されました。

- 発表・報道によれば、8月下旬、同大学職員あてに「メールボックスがいっぱいです」「重要な未配信メッセージがあります」等の警告メールが届き、3人の職員がそこから大学のサイトに偽装したフィッシングサイトに誘導され、アカウント情報を奪取されたとのことです。

- その後、職員のメールアドレスから数日間に計約16万通のメールが送信されたことにより、詳細を調査した結果、サーバから個人情報がダウンロードされていたことが発覚しています。

サイバーセキュリティ.com

ニュースの概要

関西学院大学は2016年10月7日、大学のサイトを装ったメールを受信した理工学部の職員が偽サイトに誘導され、大学院生ら1466人の個人情報が流出したと発表した。

同職員は8月23日、重要性を謳ったメールに気づき、添付されていたURLにアクセス。学内のサイトを装った偽サイトに誘導され、それがフィッシングサイトだと気づかないままIDとパスワードを入力してしまい、情報を盗み取られた。

9月7日に、同職員のメールアドレスから大量のメールが送信されていたことが発覚し、大学が調べたところ、理工学研究科の院生や卒業生らの氏名や生年月日、住所、電話番号などの個人情報が流出していることがわかったという。

その後の対応

同大では、情報を悪用されたという報告はないというが、該当する学生らに謝罪。学内の情報環境機構を中心に教職員に注意喚起をするとともに、再発防止を徹底するとしており、兵庫県警にも被害を報告しているという。

考察

最近のフィッシングサイトは本物のWebページのテキストや画像などを使い、見かけが本物ように見えるのはもちろんのこと、URLを本物のドメインと同じ綴りを含めて作っていたりと、巧妙な手口が増えている。

AUS便りからの所感等

- 情報によれば、特に8月以降に、複数の大学を装ったフィッシングが発生している模様で、各大学から主に学内向けに警告が出ており、正規のサイトのデザインについて画像で示すとともに、URL等から正規のサイトであることを確認するよう呼び掛けています。

- 当便りでは、フィッシングへの対策として、たびたび、アンチウイルス・UTM・Webブラウザのフィッシング対策機能の活用と、正規サイトへのブックマークからのアクセスを推奨していますが、サービス管理者の視点でも、今日におけるフィッシングの実情を鑑みると、可能な限りメールにURLを記載して誘導するやり方は控え、やはり正規のサイトのブックマークを促すべきと考えます。