— AUS（アルテミス・ユーザ・サポート）便り 2016/10/11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。

●JPEG 2000画像処理ライブラリに脆弱性、PC乗っ取り等の可能性

http://japan.zdnet.com/article/35089976/
http://internet.watch.impress.co.jp/docs/news/1023275.html

このニュースをザックリ言うと・・・

- 9月30日（現地時間）、米Cisco社のセキュリティ部門Talosより、JPEG 2000(※)画像を処理するライブラリ「OpenJPEG」に脆弱性が存在することが発表されました。
- JPEG 2000はJPEGの後継として規格化された画像フォーマットであり、PDFファイルへの画像埋め込み等で用いられています。
- 発表によれば、リモートの攻撃者が細工した不正なJPEG 2000画像をユーザに読み込ませることにより、任意のコードを実行される可能性があるとされています。

AUS便りからの所感等

- JPEG 2000は良く知られているJPEGより画質や圧縮率が向上していることが特徴ですが、殆どのWebブラウザにおいて未対応である等、JPEG画像を置き換えるにはまだ至っていません。
- 一方で、前述したPDFの他、ネットワークカメラ等、JPEG 2000の存在を意識しない場面で多く用いられているとされており、このことから、Webブラウザ上からネットワークカメラの映像を見るためのプラグインが狙われる可能性もあります。
- OpenJPEGについては対策バージョン2.1.2がリリースされていますが、JPEG 2000を取り扱う各種ソフトウェアがアップデートするまでの間に脆弱性を突かれることがないよう、アンチウイルスやUTMによる防御を固めてください。

ZDNet Japan

「OpenJPEG」に脆弱性--遠隔地からのコード実行を許す可能性

Charlie Osborne （ZDNet.com） 翻訳校正： 編集部 2016年10月04日 11時17分

Cisco Talosの研究者らは米国時間9月30日、OpenJPEGの「JPEG 2000コーデック」に深刻な脆弱性を発見していたことを発表した。この脆弱性が悪用されれば、遠隔地からの攻撃によって任意のコードを実行される可能性があるという。

この脆弱性（CVE-2016-8332）は、OpenJPEGライブラリ内の、JPEG 2000の画像ファイル形式を解析する実装で、ヒープ領域の境界を越えた書き込み（Out-Of-Bounds Write）を許すというものだ。こういった領域外への書き込みによって、ヒープの破壊がもたらされたり、任意のコードの実行を許してしまう可能性がある。

OpenJPEGとはC言語によって書かれたオープンソースのJPEG 2000コーデックのこと。PopplerやMuPDF、PdfiumソフトウェアなどでPDFファイル内に画像フォーマットを埋め込む際などに広く使われている画像圧縮標準JPEG 2000を推進するために作られた。

共通脆弱性評価システム（CVSS）のスコアで7.5と評価されたこの脆弱性は、JPEG 2000形式のファイル内に存在するMCC（Multiple Component Collection）レコードの解析時に発生したエラーによって、「ヒープ領域に隣接したメモリに対する不正な読み込みや書き込み」が引き起こされるというものだ。こういった誤動作を悪用すると、ヒープ領域のメタデータプロセス上でのメモリ破壊を発生させることができる。

INTERNET Watch

オープンソースのJPEG 2000コーデック「OpenJPEG」に脆弱性、Cisco Talosが報告

岩崎 宰守　2016年10月4日 18:37

米Ciscoのセキュリティチームであるcisco Talosは9月30日、オープンソースのJPEG 2000コーデックである「OpenJPEG」のライブラリに脆弱性を発見していたことを公表した。

脆弱性「CVE-2016-8332」は、OpenJPEGライブラリのバージョン2.1.1におけるJPEG2000ファイルパーサーにおけるもので、JPEG2000画像のMCC（Multiple Component Collection）レコードを解析する際に、ヒープ領域を越えたメモリへのデータ書き込み（Out-Of-Bounds Write）が可能になるもの。

この脆弱性を悪用すると、細工されたJPEG 2000の画像ファイルを開かせることで、リモートから任意のコードが実行される可能性がある。共通脆弱性評価システム（CVSS）のスコアは7.5。

Cisco Talosによれば、画像ファイルをメールに添付したり、「Google Drive」や「Dropbox」といった一般的なクラウドストレージサービスからダウンロードさせるといった手法で脆弱性を悪用できるとしている。

OpenJpegライブラリはJPEG2000規格のリファレンス実装で、「poppler」「MuPDF」「Pdfium」といったPDFレンダラーでも利用されている。

(※)JPEG2000（ジェーペグにせん） IT用語辞典 e-Words
JPEG2000とは、画像圧縮方式の一つでJPEGを発展させた仕様。画像符号化の標準化を行うISOとITU-TSの共同組織、JPEG（Joint Photographic Experts Group）によって2001年1月に規格化された。
前身のJPEGは、1990年に制定された静止画の圧縮・展開に関する国際標準規格で、ISO 10918-1（ITU-TS T.81）として規格化されている。
JPEG2000は静止画像の圧縮・展開の方式を定めた規格で、従来のJPEGよりも高圧縮、高品質な画像圧縮が行えるのが特徴。
従来のJPEG方式では画像を離散コサイン変換（DCT:画像を小さなブロック分割して周波数成分係数を量子化・符号化して圧縮する方式）で変換するが、JPEG2000ではウェーブレット変換（ウェーブレット関数により画像全体を周波数帯域に分けた縦横それぞれの周波数成分を量子化・符号化して圧縮する方式）で変換する。
このため、JPEGでは高圧縮率（低画質）で保存したときに目立っていたブロックノイズ（格子状ノイズ）やモスキートノイズ（水面の波紋状のノイズ）が、JPEG2000では発生しない。また、「電子透かし」の挿入や、圧縮する際の画質、ファイルサイズなどの細かい指定が可能となっている。

●BINDの脆弱性を狙う攻撃発生を確認、警察庁など注意喚起

https://www.npa.go.jp/cyberpolice/topics/?seq=19301

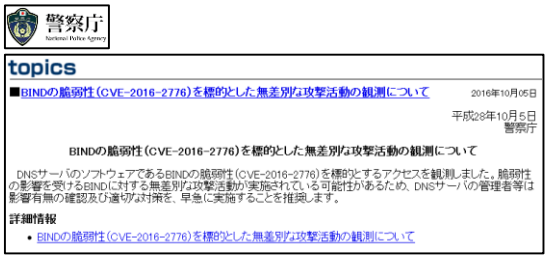
このニュースをザックリ言うと・・・

- 10月5日（日本時間）、警察庁より、9月27日に発表されたDNSサーバソフト「BIND」の脆弱性（「AUS便り 2016/10/03号」参照）を突く無差別攻撃が確認されたとして警告が出されています。

- 10月3日の時点で、情報処理推進機構（IPA）から脆弱性に対する攻撃コードが公開されていると発表があり、警察庁によれば、10月4日の18時以降に、この攻撃コードによるとみられる攻撃パケットを観測したとのことです。

- 警察庁では、運用中のDNSサーバが脆弱性を受けるバージョンのBINDであるかを早急に確認して、最新版へのアップデートを行うこと等を呼び掛けています。

AUS便りからの所感等


警察庁
topics
■BINDの脆弱性（CVE-2016-2776）を標的とした無差別な攻撃活動の観測について 2016年10月05日
平成28年10月5日
警察庁
BINDの脆弱性（CVE-2016-2776）を標的とした無差別な攻撃活動の観測について
DNSサーバのソフトウェアであるBINDの脆弱性（CVE-2016-2776）を標的とするアクセスを観測しました。脆弱性の影響を受けるBINDに対する無差別な攻撃活動が実施されている可能性があるため、DNSサーバの管理者等は影響有無の確認及び適切な対策を、早急に実施することを推奨します。
詳細情報
• BINDの脆弱性（CVE-2016-2776）を標的とした無差別な攻撃活動の観測について

- DNSでは主にUDPが利用されており、攻撃パケットが送信元IPアドレスを偽装することも珍しくありません（やはりUDPを用いるNTPやTFTPでは、IPアドレスを偽装したパケットによるDDoS攻撃が発生したこともあります）。

- このようなことから、警察庁の発表では、BINDの設定に依存したアクセス制限による回避策は実施しないようにともあります。

- 今回確認された攻撃パケットのサイズはわずか500バイト強となっており、2003年にMicrosoftのSQL Serverの脆弱性を突いて感染するワーム「SQL Slammer」が猛威を振るったことがあり、こちらもワームの本体は1つのUDPパケットに収まる小さいものでした。

- とにかく、BINDのアップデートによる根本的な対策は必須であり、またUTM等アプライアンスにおいてBINDを使用しているケースもあることから、こちらについてもベンダー情報を随時確認ないし問合せを行うようにしてください。

●雑貨通販サイトの個人情報38,313件が流出の疑い

http://www.tsuhannews.jp/?p=26022

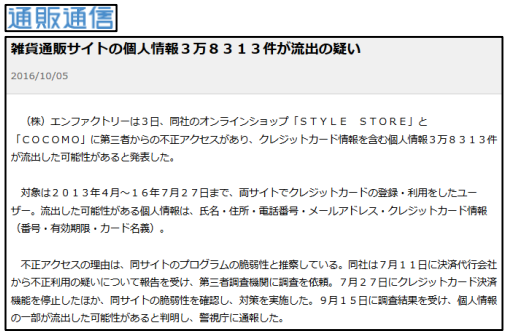
このニュースをザックリ言うと・・・

- 10月3日（日本時間）、エンファクトリー社より、同社が運営するオンラインショップ「STYLE STORE」と「COCOMO」が不正アクセスを受け、個人情報38,313件が流出した可能性があると発表されました。

- 発表によれば、流出の疑いのある情報は、2013年4月～2016年7月27日に両サイトでクレジットカードの登録・利用をしたユーザの氏名・住所・電話番号・メールアドレスおよびクレジットカード情報（番号・有効期限・名義）とされています。

- 同社では、問題となったプログラムの脆弱性を修正した他、クレジットカード決済について、クレジットカード情報が同社のサーバを通過しない「非通過型タイプ」への変更作業を行っているとしています。

AUS便りからの所感等


通販通信
雑貨通販サイトの個人情報３万８３１３件が流出の疑い
2016/10/05
（株）エンファクトリーは3日、同社のオンラインショップ「ＳＴＹＬＥ　ＳＴＯＲＥ」と「ＣＯＣＯＭＯ」に第三者からの不正アクセスがあり、クレジットカード情報を含む個人情報３万８３１３件が流出した可能性があると発表した。
対象は２０１３年４月～１６年７月２７日まで、両サイトでクレジットカードの登録・利用をしたユーザー。流出した可能性がある個人情報は、氏名・住所・電話番号・メールアドレス・クレジットカード情報（番号・有効期限・カード名義）。
不正アクセスの理由は、同サイトのプログラムの脆弱性と推察している。同社は７月１１日に決済代行会社から不正利用の疑いについて報告を受け、第三者調査機関に調査を依頼。７月２７日にクレジットカード決済機能を停止したほか、同サイトの脆弱性を確認し、対策を実施した。９月１５日に調査結果を受け、個人情報の一部が流出した可能性があると判明し、警視庁に通報した。

- クレジット取引セキュリティ対策協議会が取りまとめた「クレジットカード取引におけるセキュリティ対策の強化に向けた実行計画」において、EC事業者は、2018年3月末までに、カード情報を保持しないシステムとする、またはPCIDSSに準拠することが要求されています。

- クレジットカード情報に限らず、重要な情報を可能な限り自前のシステムで保持しないことは、万が一の不正アクセス等による流出の被害を最小限に抑えるために重要なことです。

- 現在のシステムで収集・保持している各種情報の種類について見直しを図り、不要な情報を破棄していくこと等も検討するとともに、最小限の情報を外部から、あるいは内部に感染したマルウェアから防御するよう、UTM等を有効に活用したシステム・ネットワーク構成とすることを推奨致します。