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。

●「BIND 9」全バージョンに深刻なDoS脆弱性、パケット1つでDNSサーバ異常終了の恐れ

http://internet.watch.impress.co.jp/docs/news/1022227.html
https://www.jpcert.or.jp/at/2016/at160037.html

このニュースをザックリ言うと・・・

- 9月27日（日本時間）、DNSサーバソフト「BIND」について2件の脆弱性（CVE-2016-2776）が発表され、開発元の米ISCより修正バージョン（BIND 9.10.4-P3/9.9.9-P3）がリリースされています。

- これを受けて翌9月28日には、JPCERT/CC（一般社団法人JPCERTコーディネーションセンター）やJPRS（株式会社日本レジストリサービス）等から警告が出されています。

- 脆弱性は、細工されたDNS問合せパケットを1個受信するだけでもDNSサーバプロセス（named）を不正に落とされる可能性があり、BIND 9.0.0以降全てのバージョンに影響するため、BINDをDNSサーバとして利用しているあらゆる組織、サービスについて早急なアップデートが推奨されています。

AUS便りからの所感等

- 脆弱性は、DNS権威サーバ（自組織のドメイン情報を外部に提供するサーバ）およびDNSキャッシュサーバの両方に影響するとされています。

- 前者のケースは当然危険ですが、後者において、BINDの設定でキャッシュサーバの使用を許可するIPアドレスを制限している場合でも、それ以外のIPアドレスからの攻撃パケットがDNSサーバプロセスに到達するとやはり影響を受けます。

- UTMにおいて不正なパケットを遮断してくれるようになる可能性もありますが、BINDによるDNSサーバを立てている場合は必ず最新バージョンへのアップデートを行ってください。

INTERNET Watch

ニュース

「BIND 9」全バージョンに深刻なDoS脆弱性、パケット1つでnamed異常終了

永沢 茂　2016年9月28日 15:30

Internet Systems Consortium（ISC）が開発・提供するDNSソフト「BIND 9」において、実装上の不具合により、サービス運用妨害（DoS）攻撃に悪用可能な脆弱性（CVE-2016-2776）があったとして、一般社団法人JPCERTコーディネーションセンター（JPCERT/CC）や株式会社日本レジストリサービス（JPRS）が28日、注意喚起を出した。この脆弱性を修正したバージョン「9.10.4-P3」「9.9.9-P3」がISCから27日にリリースされており、BIND 9の運用者に対して、これら修正済みバージョンへの更新または各ディストリビューションベンダーからリリースされる更新の適用を速やかに実施するよう推奨している。

脆弱性の影響を受けるのは、下記のバージョン。「9.0.0」以降のすべてのバージョンが影響を受け、すでにサポートが終了していて修正パッチがリリースされない9.8以前の系列も含まれる。

・9.11系列：9.11.0a1～9.11.0rc1
・9.10系列：9.10.0～9.10.4-P2
・9.9系列：9.9.0～9.9.9-P2
・9.0系列～9.8系列：9.0.x～9.8.x

JPCERT CC®
Japan Computer Emergency Response Team Coordination Center

ISC BIND 9 サービス運用妨害の脆弱性（CVE-2016-2776）に関する注意喚起　最終更新: 2016-09-28

各位

JPCERT-AT-2016-0037
JPCERT/CC
2016-09-28

<<< JPCERT/CC Alert 2016-09-28 >>>

ISC BIND 9 サービス運用妨害の脆弱性（CVE-2016-2776）に関する注意喚起
https://www.jpcert.or.jp/at/2016/at160037.html

I. 概要

ISC BIND 9 には、サービス運用妨害（DoS）の原因となる脆弱性があります。脆弱性を悪用された場合、リモートからの攻撃によって named が終了する可能性があります。脆弱性の詳細については、ISC 社の情報を確認してください。

Internet Systems Consortium, Inc. (ISC)
CVE-2016-2776: Assertion Failure in buffer.c While Building Responses to a Specifically Constructed Request
https://kb.isc.org/article/AA-01419/

影響を受けるバージョンの ISC BIND 9（権威 DNS サーバ、キャッシュ DNS サーバ）を運用している場合は、「III. 対策」を参考に、修正済みバージョンの適用について検討してください。

II. 対象

ISC 社の情報によると、以下のバージョンが本脆弱性の影響を受けます。
ISC 社は、本脆弱性の深刻度を、「高（High）」と評価しています。

●企業サーバからアカウント情報12万件奪取･･･高校生2人書類送検

http://www.chibanippo.co.jp/news/national/354487
http://www.kahoku.co.jp/tohokunews/201610/20161001_13026.html

このニュースをザックリ言うと･･･

- 9月30日（日本時間）、宮城県警より、不正アクセス禁止法違反などの疑いで千葉県成田市の高校生2人を書類送検したことが発表されました。

- 発表によれば、2人は2015年5月から11月にかけて企業3社のサーバに不正アクセスし、ユーザアカウント情報約12万件を奪取、また情報を悪用し、ネットショッピングでスマートフォン・ゲームソフト等計約27万円分を不正に購入したとされています。

千葉日報

ＩＤ１２万件取得の疑い　成田の高１、２人書類送検　宮城県警

2016年10月1日 07:27 | 無料公開

宮城県警は３０日、企業のサーバーに侵入して約１２万件のＩＤとパスワードを取得したなどとして、不正アクセス禁止法違反などの疑いで、いずれも成田市の１６歳と１５歳の高校１年の少年２人を書類送検した。

県警によると、２人は同じ中学校に通っていた友人同士で、１６歳の少年は「将来ハッカーになりたかった」と供述。取得した個人情報を使い、インターネットショッピングでスマートフォンやゲームソフトなど計約２７万円分を買ったという。

１６歳の少年の送検容疑は昨年５～１１月、企業３社が管理するサーバーに不正にアクセスし、他人のＩＤとパスワード約１２万件を取得した疑い。１５歳の少年は同１１月下旬、１６歳の少年と共に、取得したＩＤなどを使って、大手ショッピングサイトのサーバーに侵入したとされる。

昨年８月、ネットショッピングを利用する仙台市青葉区の女性会社員から「身に覚えのない買い物履歴がある」と警察に届けがあり、発覚した。

河北新報 ONLINE NEWS

「ハッカーになりたかった」高１を書類送検

企業のサーバーに侵入して入手したＩＤやパスワードで楽天市場などに不正アクセスしたとして、宮城県警は３０日、不正アクセス禁止法違反などの疑いで、千葉県成田市の１６歳の高校１年の少年を書類送検した。

県警によると、少年は「将来、ハッカーになりたかった」と供述。不正に入手したＩＤとパスワードは約１２万件に上り、インターネットショッピングでスマートフォンやゲームソフトなど９点（約２７万円相当）を手に入れたという。

パソコンやスマートフォンなどの押収品

AUS便りからの所感等

- 高校生による不正アクセス事件としては、佐賀県の高校生が同県の学校教育ネットワークに侵入し、個人情報約9600人分等を奪取した事件（AUS便り 2016/07/04号参照）が一例として挙げられます。

- 一部報道によれば、今回の件では「SQLインジェクション」の脆弱性を突いて個人情報を奪取したものとされており、このような危険度が高く、かつ良く知られた脆弱性は、企業規模の大小に拘らずあらゆる攻撃者からターゲットとされる恐れがあります。

- 脆弱性の有無を確認し、速やかに対策できる体制を整え、一方で不正アクセスを適切に検知・遮断できるようなシステム・ネットワーク構成になっているかを確認し、UTMの設置を含めた見直しを随時行っていくことが重要です。

●「郵便受けにUSBメモリ」がマルウェアの新たな感染経路に･･･ランサムウェア感染の実例も

http://www.itmedia.co.jp/news/articles/1609/23/news106.html

このニュースをザックリ言うと･･･

- 9月22日（現地時間）、米AP通信により、USBメモリを用いた新たなマルウェア拡散の可能性に関する出来事が取り上げられました。

- 記事によれば、今年7月、フランス在住のソフトウェアエンジニアの男性宅のポストに切手や宛先等のない不審な封筒が投函され、中にはUSBメモリが入っていたとのことで、男性はUSBメモリをそのまま処分し、その写真をTwitterに投稿し「こういうプレゼントは絶対に差し込んだらダメ」とコメントしています。

- また、9月21日にはオーストラリア警察が「メルボルンの南東約60キロに位置するパケナムにおいて『極めて有害』なUSBメモリが郵便受けに入れられる事例が相次いでいる」と発表し、AP通信の取材に対し、「印字のないUSBメモリが届いた」という報告が数日前から寄せられるようになったと語っています。

- なお、USBメモリには、動画配信サービスのクーポンに偽装したランサムウェアが入っていた模様で、被害も数件発生しているとのことです。

ITmedia ニュース

速報　2016年09月23日 17時12分 更新

「郵便受けにUSBメモリ」がマルウェアの新たな感染経路に(1/2)

USBメモリの投げ込みにご注意を。

[AP通信]

ジュリアン・アスコエトさんは今年7月、郵便受けから無地の白い封筒を取り出した時点で既に不審に思っていたという。

封筒には切手は貼られておらず、何の印字もなかった。フランス北西部の港町ナントの郊外に住むアスコエトさんの自宅に何者かが直接届けたにちがいない。

ソフトウェアエンジニアのアスコエトさんは9月22日、オンラインチャットで次のように語った。「何が入っているか分からないので、恐るおそる封を開けた。刑事ドラマ『NCIS』で、似たような封筒に炭疽菌が入っていたエピソードを思い出していた」

AUS便りからの所感等

- 2015年、米イリノイ大学で行われた実験では、放置された約300個のUSBメモリの約半数が拾われてPCに接続されたという結果が出ています（AUS便り 2016/05/02号参照）。

- USBの仕様上、単にUSBメモリを接続しただけでもデバイスドライバに偽装したマルウェアが実行される恐れがあり、今後OS側等でUSBデバイスを安全に取り扱うセキュリティ機能が確立されることも考えられますが、現時点では「出所が不明なUSBデバイスは接続しないこと」「アンチウイルスによる感染防御」あるいは「UTMによる出口対策」といった防御策を必ずとることが肝要です。