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。

●Webサーバーの設定ミスか…メールサービス利用者のアドレス、受信メールが公開状態に

https://krebsonsecurity.com/2024/02/u-s-internet-leaked-years-of-internal-customer-emails/

このニュースをザックリ言うと・・・

- 2月14日(現地時間)、米セキュリティ情報サイトKrebs on Security(以下・Krebs)より、米国のISPであるU.S.Internet社が提供するメールフィルタリングサービス「Securence」の利用者のメールアドレスおよびメールそのものが外部から参照可能な状態になっていたと発表されました。

- Krebsに情報を提供したセキュリティ企業によれば、Securenceに関するWebサーバーへのアクセスにより、ディレクトリリストが表示され、ディレクトリ名からSecurenceの利用者とみられるドメイン名やメールアドレスが読み取れたとしています。

- 利用者は企業から教育機関・政府機関にまで及び、さらに各メールアドレスのディレクトリ内において、そのアドレスに届いたメールを読むことも可能だったとしています。

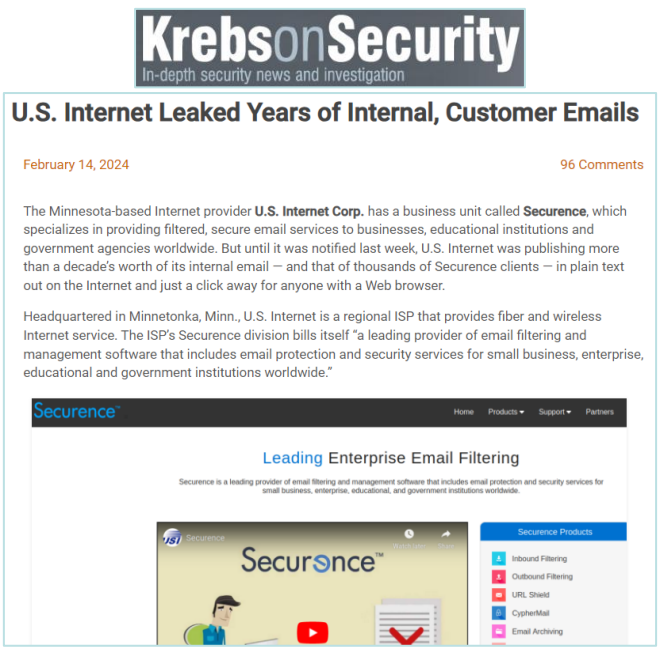
- KrebsではU.S.Internet社に連絡をとり、現在はディレクトリは非公開になったとしています。

AUS便りからの所感等

- 今回のケースは、Webサーバー「Nginx」においてIMAPプロキシーサーバー機能を設定した際に問題があったとされており、本来はインターネット上からアクセスできない内部サーバーとして設定される前提だったものと推測されます。

- 90年代～2000年代には、例えば個人情報やWebフォームから入力されたアンケート回答のデータ等を含むファイルがWebサイトのドキュメントルート(DocumentRoot)以下に保存されることにより、外部から閲覧可能な状態にあったケースが頻繁に報告されていました(今回のように、ディレクトリ情報が表示される設定になっていたために、そういったデータが保存されているディレクトリが見つけやすい状態にあったケースも珍しくありません)。

- 機密情報に対する第三者からのアクセスを防ぐため、内部サーバーへ外部からアクセスされないよう適切な配置およびファイアウォールやサーバー自体のフィルタリングをはじめセキュアな設定を行うことはもちろん、実施した設定が機能しているかの確認のため、サーバーやディレクトリを指定し、実際にアクセスしてチェックすること(IPアドレスベースでの制限時は許可された以外のアクセス元からアクセスすること)が重要です。


KrebsonSecurity
In-depth security news and investigation

U.S. Internet Leaked Years of Internal, Customer Emails

February 14, 2024 96 Comments

The Minnesota-based Internet provider **U.S. Internet Corp.** has a business unit called **Securence**, which specializes in providing filtered, secure email services to businesses, educational institutions and government agencies worldwide. But until it was notified last week, U.S. Internet was publishing more than a decade's worth of its internal email — and that of thousands of Securence clients — in plain text out on the Internet and just a click away for anyone with a Web browser.

Headquartered in Minnetonka, Minn., U.S. Internet is a regional ISP that provides fiber and wireless Internet service. The ISP's Securence division bills itself "a leading provider of email filtering and management software that includes email protection and security services for small business, enterprise, educational and government institutions worldwide."

●DNSサーバー「BIND」に7件の脆弱性、DoS攻撃等の可能性あり

https://jvn.jp/vu/JVNVU92131687/
https://www.jpcert.or.jp/newsflash/2024021401.html
https://jprs.jp/tech/

このニュースをザックリ言うと･･･

- 2月14日(日本時間)、DNSサーバー「BIND」に7件の脆弱性が発見されたとして、修正バージョン(9.18.24/9.16.48等)がリリースされました。

- 一般的に利用されるバージョンには影響しない1件を除いた6件はいずれも危険度が高いものとされ、BINDのサーバープロセスを不正にダウンさせられる、あるいはBINDが動作しているサーバーのパフォーマンスを低下させられるといった、外部からのDoS攻撃に繋がり得るものとなっています。

- JPCERT/CC等からも脆弱性についての注意喚起が出されており、可能な限り速やかなアップデートが推奨されています。

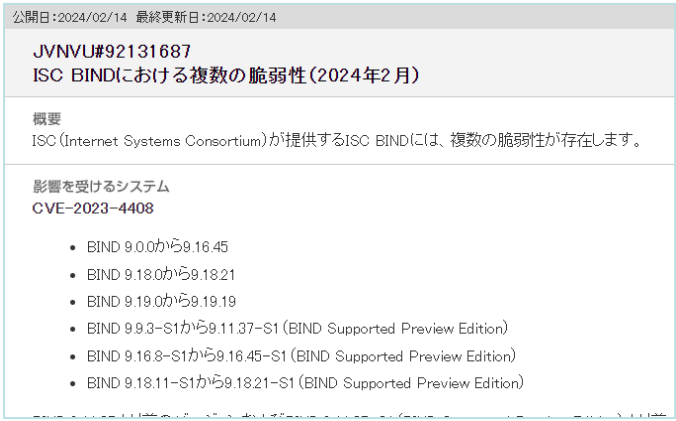
- また、今回報告された脆弱性の一部は、BIND以外のキャッシュDNSサーバーであるUnbound・Knot Resolver・PowerDNS RecursorおよびWindows ServerのDNSサービスについても影響するとされ、それぞれセキュリティアップデートがリリースされています。

AUS便りからの所感

- BINDは最も有名なDNSサーバーソフトウェアとされる一方、長年の間多くの脆弱性が報告されているソフトウェアでもあります。

- 2/21現在での各Linuxディストリビューションにおけるアップデートのリリース状況はまちまちで、Debian・Ubuntuからはアップデートがリリースされている一方、RHELおよび派生ディストリビューション(CentOS7・Rocky Linux・Almalinux等)についてはまだリリースされていない模様です。

- BINDの代替として他のソフトウェアを使用するケースも多くなっているものの、今回のようにそれらのソフトウェアにも影響する脆弱性があること、またメーカー製ネットワーク機器においてBINDを組み込んでいるケース等にも影響し得ることを鑑み、使用しているソフトウェア・機器のファームウェアについて脆弱性の有無やアップデートのリリース状況を随時確認すること、リリースされ次第適用を行うことが肝要です。



公開日:2024/02/14 最終更新日:2024/02/14

JVNVU#92131687
ISC BINDにおける複数の脆弱性(2024年2月)

概要
ISC(Internet Systems Consortium)が提供するISC BINDには、複数の脆弱性が存在します。

影響を受けるシステム
CVE-2023-4408

- BIND 9.0.0から9.16.45
- BIND 9.18.0から9.18.21
- BIND 9.19.0から9.19.19
- BIND 9.9.3-S1から9.11.37-S1 (BIND Supported Preview Edition)
- BIND 9.16.8-S1から9.16.45-S1 (BIND Supported Preview Edition)
- BIND 9.18.11-S1から9.18.21-S1 (BIND Supported Preview Edition)

●リスト型攻撃でメールアカウントに不正ログイン、フィッシングメール3万件送信

https://www.huhp.hokudai.ac.jp/?p=13758

このニュースをザックリ言うと･･･

- 2月2日(日本時間)、北海道大学病院より、同病院職員のメールアカウントが外部から不正にログインされたと発表されました。

- 不正ログインは2023年12月27日に判明したもので、外部へのフィッシングメール約3万件の送信に悪用されたとしていますが、第三者によるメールの閲覧等はなく、個人情報漏洩の可能性はないとしています。

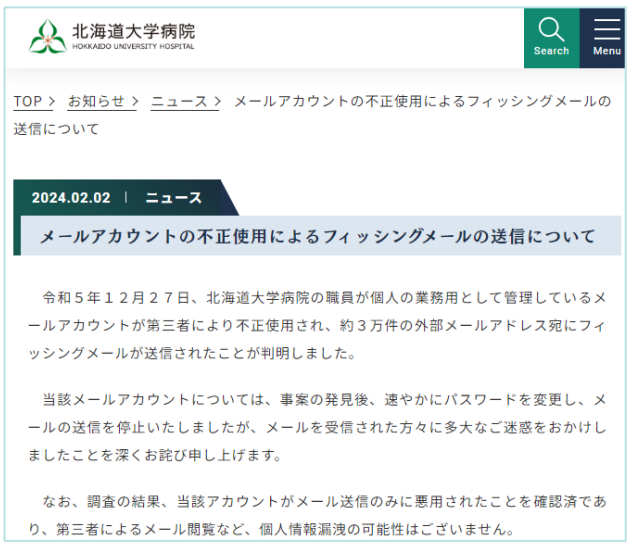
- 外部サービスで流出したアカウント・パスワード情報を用いた、いわゆる「リスト型攻撃」によってログインされたもので、パスワード変更によりメール送信を停止したとしています。

AUS便りからの所感

- メールアカウントへの不正ログインは、今回は発生しなかった受信メールを閲覧される可能性の他、元のユーザー・組織になりすましてのメール送信が行われた場合、SPF・DKIM・DMARCといった各種フィッシング対策機構による確認が通用しなくなる恐れがあります。

- 今回のケースはリスト型攻撃、即ち別のサービスとパスワード等を使い回していたことが原因で不正ログインに至ったとされ、全てのアカウントで異なる、かつ推測しにくいパスワードを設定することがアカウント保護のための大原則です。

- 一方で、クライアントPCにマルウェア等が侵入してアカウント情報を奪取されたり、そこからフィッシングメールを送信されたりするシナリオも多く発生しており、メールアカウントの厳密な管理以外にも、アンチウイルスによるPCの保護は必要不可欠ですし、加えてUTMによる社内LANから外部への不審なメール送信の遮断、メールサーバー上で不正なログイン試行を遮断する設定等も検討に値します。



北海道大学病院 HOKKAIDO UNIVERSITY HOSPITAL
Search Menu

TOP > お知らせ > ニュース > メールアカウントの不正使用によるフィッシングメールの送信について

2024.02.02 | ニュース

メールアカウントの不正使用によるフィッシングメールの送信について

令和５年１２月２７日、北海道大学病院の職員が個人の業務用として管理しているメールアカウントが第三者により不正使用され、約３万件の外部メールアドレス宛にフィッシングメールが送信されたことが判明しました。

当該メールアカウントについては、事案の発見後、速やかにパスワードを変更し、メールの送信を停止いたしましたが、メールを受信された方々に多大なご迷惑をおかけしましたことを深くお詫び申し上げます。

なお、調査の結果、当該アカウントがメール送信のみに悪用されたことを確認済であり、第三者によるメール閲覧など、個人情報漏洩の可能性はございません。