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。

●大手家具ストアアプリに「リスト型攻撃」による不正ログイン…ユーザー約132,000件の個人情報流出か

https://internet.watch.impress.co.jp/docs/news/1441843.html
https://www.nitori-net.jp/ecstatic/image/pdf/nitori001.pdf
https://www.nitorihd.co.jp/news/items/2cdbc59fa4c3ffe4da790cc1cfe85200.pdf
https://www.nitorihd.co.jp/news/items/72a9f692d27769ef90c0fc86d9c7d6d5.pdf

このニュースをザックリ言うと･･･

- 9月20日(日本時間)、ニトリホールディングス社より、同社のスマートフォンアプリ「ニトリアプリ」に対する不正ログインが発生していたことが発表されました。

- 不正ログインの対象とされるのは、ニトリネット・ニトリアプリ・シマホアプリで会員登録を行った、あるいはシマホネットでニトリポイント利用手続きを行ったユーザー約132,000件で、個人情報(メールアドレス・パスワード・会員番号・氏名・電話番号・住所等)が第三者に閲覧された可能性があるとのことです。

- 不正ログインは9月15日から発生、同19日になって同社で攻撃の存在を確認、外部サービスから流出したアカウント情報のリストによる、いわゆる「リスト型攻撃」の可能性があるとしており、対象ユーザーについてパスワードのリセットを行っているとのことです。

AUS便りからの所感等

- クレジットカード番号の一部と有効期限も第三者に閲覧された可能性があるものの、カード決済に必要な情報は同社グループのシステム上に保持されていないため、クレジットカード決済が実行されることはないとしています。

- リスト型攻撃は不正ログインのターゲットとなるサイトのシステム自体の脆弱性等を突かなくとも成立し得るものであり、ユーザー側はその被害を受けないよう、「複数のサイト等で同じパスワードを使い回さない」「推測されにくいパスワードを設定する(場合によってはパスワード管理ツールの利用も検討する)」という鉄則を改めて認識・実行することが肝要です。

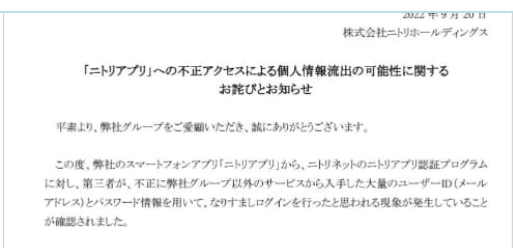
- 一方で、リスト型攻撃による不正ログインが問題視されるようになって10年近く経過し、二段階認証・多要素認証等のログイン機構を強化する方法が普及している現状、サービス提供者側においても、パスワードの設定における対策をユーザーに呼び掛けるアプローチだけに留まらず、多要素認証の導入等による積極的なユーザーの保護が今後要求されることになるでしょう。

Impress Watch

「ニトリアプリ」にリスト型攻撃と推測される不正ログイン、約13万2000件の個人情報流出の可能性

当該ユーザーはパスワードをリセットし、メール連絡

林 恭平　2022年9月22日 12:21



2022年9月20日
株式会社ニトリホールディングス

「ニトリアプリ」への不正アクセスによる個人情報流出の可能性に関するお詫びとお知らせ

平素より、弊社グループをご愛顧いただき、誠にありがとうございます。

この度、弊社のスマートフォンアプリ「ニトリアプリ」から、ニトリネットのニトリアプリ認証プログラムに対し、第三者が、不正に弊社グループ以外のサービスから入手した大量のユーザーID（メールアドレス）とパスワード情報を用いて、なりすましログインを行ったと思われる現象が発生していることが確認されました。

株式会社ニトリホールディングスは9月20日、同社のスマートフォンアプリ「ニトリアプリ」に対する不正ログインを確認したと発表した。

ニトリアプリのニトリネット認証プログラムに対して、大量のユーザーID（メールアドレス）とパスワード情報を用いたなりすましログインを確認したという。不正ログインの手法は、ニトリグループ以外のサービスから流出したユーザーIDとパスワード情報を用いた、「リスト型アカウントハッキング（リスト型攻撃）」だと推測している。

● DNSサーバー「BIND」に6件の脆弱性、DoS攻撃等の可能性あり

https://jvn.jp/vu/JVNVU90776782/index.html

このニュースをザックリ言うと・・・

- ９月21日（現地時間）、DNSサーバー「BIND」に6件の脆弱性が発見されたとして、修正バージョン(9.19.5/9.18.7/9.16.33)がリリースされました。

- 6件の脆弱性の多くは、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おり、この他にサーバープロセスのメモリ領域の読み取りによる情報漏洩の可能性も存在するとのことです。

- 米CISAや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。

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。

- 現時点(9/27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ではリリースされている一方、CentOSについてはまだリリースされていません(ディストリビューションやそのバージョン次第で、6件の脆弱性それぞれが影響するか否かも様々です)。

- また、BIND以外のキャッシュDNSサーバーであるUnbound・Knot Resolverについても、相次いでDoS攻撃の脆弱性が報告されており、使用しているソフト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。

JVNVU#90776782
ISC BINDにおける複数の脆弱性

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-2022-2795

- BIND 9.0.0から9.16.32まで
- BIND 9.18.0から9.18.6まで
- BIND 9.19.0から9.19.4まで
- BIND 9.9.3-S1から9.11.37-S1まで(BIND Supported Preview Edition)
- BIND 9.16.8-S1から9.16.32-S1まで(BIND Supported Preview Edition)

CVE-2022-2881、CVE-2022-2906

- BIND 9.18.0から9.18.6まで
- BIND 9.19.0から9.19.4まで

CVE-2022-3080

- BIND 9.16.14から9.16.32まで
- BIND 9.18.0から9.18.6まで

●日本赤十字社を騙るフィッシング、対策協議会等が注意喚起

https://www.antiphishing.jp/news/alert/jrc_20220920.html
https://www.jrc.or.jp/information/2022/0920_028508.html

このニュースをザックリ言うと・・・

- 9月20日(日本時間)、日本赤十字社を騙るフィッシングが確認されたとして、同社やフィッシング対策協議会より注意喚起が出されています。

- 対策協議会が挙げているフィッシングメールの例は、件名が「【COVID-19】コロナ対策、慈善寄付」、本文が「日本赤十字社新型コロナウイルス感染症に対する活動報告」という赤文字のタイトルで始まり、同社への寄付申込と偽って個人情報やクレジットカード情報を詐取するフォームへ誘導するものとなっています。

- 同社では9月17日～19日にフィッシングメールが発信されていたことを確認、同社とは一切関係がないものとしており、当該メールを受け取った場合はバナー等をクリックせず、メールごと削除するよう呼び掛けています。

AUS便りからの所感

- 偽フォームは日本赤十字社の本物の寄付申込サイト(https://donate.jrc.or.jp/)からコンテンツをコピーしたものとみられ、メールの文面も含め一目ではフィッシングと気づきづらいものとなっています。

- くれぐれも「フィッシングメール・サイトはどこかがそれとわかる違和感のある文面となっている」といった思い込みに囚われることなく、ブラウザー・メーラー・セキュリティソフトあるいはUTMにおけるアンチフィッシング機能を有効にしてメールやサイトのチェックを行うとともに、自身も慎重に行動するよう心掛けてください。

メール本文

日本赤十字社新型コロナウイルス感染症に対する活動報告

活動へのご理解をよろしくお願いします。

日本赤十字社は、昨年より全国の赤十字病院を中心に新型コロナウイルス感染症の治療および感染拡大防止のための活動に取り組んでおります。

医師・看護師を中心に感染者の治療にあたっている赤十字病院だけでなく、コロナまん延下での災害救護や救急搬送での傷病など、活動の内容は多岐にわたっています。

引き続き、皆さまと力を合わせて、感染防止活動を広げていきたいと思います。

ご理解、ご支援のほど、よろしくお願いいたします。

ご寄付で赤十字の活動をご支援ください

寄付で赤十字を支援する

Copyright © 2022 Japanese Red Cross Society All rights reserved.