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。

●富士通提供の情報共有ツールに不正アクセス…成田空港・省庁等情報流出相次ぐ

https://xtech.nikkei.com/atcl/nxt/news/18/10426/
https://www.itmedia.co.jp/news/articles/2105/27/news149.html
https://www.asahi.com/articles/ASP5W6KSNP5WUTIL01P.html
https://www.naa.jp/jp/news/index.html
https://pr.fujitsu.com/jp/news/2021/05/25.html

このニュースをザックリ言うと･･･

- 5月20日、成田国際空港(NAA)より、同空港の運航情報管理システムに関する情報が、当該システムで利用していた富士通製プロジェクト情報管理ツール「ProjectWEB」への不正アクセスにより、流出したと発表されました。

- 同25日には、富士通より、不正アクセスに関する正式発表があり、原因を調査するとともに、ProjectWEBの運用を停止しているとのことです。

- また同26日には、同じくProjectWEBを利用していた、内閣官房内閣サイバーセキュリティセンター(NISC)、国土交通省および外務省からも情報流出が相次いで発表されており、国交省については省内外の関係者のメールアドレス約76,000件分が流出、外務省についても一部報道によれば省外63人分の個人情報が流出したとされ、NISCでは「政府機関等、重要インフラ事業者等それぞれに向けて、同種ツールに対する不正アクセス対策の確認について注意喚起」を行ったとしています。

AUS便りからの所感等

- 複数のユーザーに提供されるクラウド型サービスにおいてこのような不正アクセスの同時多発が発生するケースとしては、他にも適切に管理されていない多数のユーザーアカウントが狙われるケース等も起こり得ますので、一般論とはなりますが、ユーザーアカウントに対し外部から容易にパスワードを推測されたりして不正ログインされることのないよう、複雑なパスワードの設定等厳密な管理を行うことは、ユーザー側・サービス提供者側の区別なく重要と言えます。

- 一部報道によれば、不正アクセスによってProjectWEBの管理者権限を持ったアカウントが侵害された可能性があると富士通から省庁に報告されたとのことですが、このような管理者アカウントの奪取をも見越し、それが直ちにシステム全体へのデータアクセスに繋がることのないようなシステムの構築もまた課題となるでしょう。

日経XTECH

成田空港駐機場管理システムの関連情報、富士通管理の情報共有ツールから流出か

横田 宏幸　日経クロステック/日経コンピュータ

2021.05.21

成田国際空港会社（NAA）は2021年5月20日、同空港内駐機場の稼働実績やスケジュールを管理する運航情報管理システム「NARCIV（ナーク フォー）」に関連する情報が、外部流出した可能性が高いと発表した。同社IT推進部は2021年5月21日、日経クロステックの取材に「運航情報管理システムは富士通が開発した。このシステムには、インターネットから接続できないため、セキュリティー上の影響は生じないと考えられる」と答えた。

NAA NARITA AIRPORT

2021年5月20日
成田国際空港株式会社
広　報　部

報道関係各位

ITmedia NEWS

富士通製ツールへの不正アクセスで複数省庁や企業の情報が流出　国交省職員のメールアドレス7.6万件も確認

2021年05月27日 19時03分 公開　[ITmedia]

印刷　367　Share　B! 24

富士通は5月25日、自社製のプロジェクト情報共有ツール「ProjectWEB」が不正アクセスを受けたと発表した。複数の省庁や企業が同ツールを利用していたことから、省庁を中心に情報流出の被害が複数報告される事態になっている。

国土交通省は5月26日、ProjectWEBが受けた不正アクセスにより、職員などのメールアドレス7.6万件が外部に流出したと発表した。既に同ツールの使用は停止しており、流出した情報の悪用は現時点で確認されていないという。

● Bluetoothに複数の脆弱性、なりすまし等の恐れ

https://news.mynavi.jp/article/20210525-1893718/
https://kb.cert.org/vuls/id/799380
https://jvn.jp/vu/JVNVU99594334/

このニュースをザックリ言うと･･･

- 5月24日(現地時間)、米CERT/CCより、多くのBluetooth機器に影響するとみられる複数の脆弱性について注意喚起が出されています。

- 脆弱性は「Bluetooth Core Specification」および「Mesh Profile Specification」をサポートする機器に存在するとされ、悪用により、ペアリング時に攻撃者が正規のデバイスになりすますこと等が可能とされています。

- CERT/CCでは、機器あるいはOSのベンダーからのアップデート提供を確認するよう推奨しています。

AUS便りからの所感

- BTについては2017年に、機器へのペアリングなしでのアクセスおよび機器の乗っ取り等が可能とされる「BlurBorne」と呼ばれる脆弱性が報告されたことがあり、先日はWi-FiについてもWPA3までの各セキュリティプロトコルについて脆弱性が報告されています(AUS便り 2021/05/17号参照)。

- CERT/CCの情報では、現時点でAndroidやLinuxについては一部影響を受けるとされますが、マイクロソフトやAppleを含め情報はまだ出揃っておらず、アップデートの提供にはまだしばらくかかりそうです。

- BTはWi-Fiに比べ通信範囲が狭い一方、機器の用途は多く、複数の機器が連鎖して攻撃を受けるケースも考えられるため、可能であれば、全ての機器に確実にアップデートが適用され、安全が確認されるまで、BT自体を使用しないことも、検討に値するでしょう。


TECHR Powered by マイナビニュース

Bluetoothになりすましの脆弱性、多くのデバイスに影響か

2021/05/25 11:31　著者：後藤大地

現在、Bluetoothはさまざまな機器で使われているが、この便利な機能に新しい脆弱性が発見された。この脆弱性を悪用されると、攻撃者によって正規のデバイスになりすまされる危険性があるという。多くのデバイスが影響を受けるおそれがあり、注意が必要だ。

CERT Coordination Center (CERT/CC： Carnegie Mellon University)は5月24日(米国時間)、「VU#799380 - Devices supporting Bluetooth Core and Mesh Specifications are vulnerable to impersonation attacks and AuthValue disclosure」において、「Bluetooth Core Specification」および「Mesh Profile Specification」をサポートするデバイスに脆弱性が存在すると伝えた。

●「電話料金が大変高額に」「発送状況を で確認ください」…ドコモ騙るフィッシングに注意喚起

https://www.itmedia.co.jp/news/articles/2105/27/news146.html
https://www.antiphishing.jp/news/alert/nttdocomo_20210527.html
https://www.nttdocomo.co.jp/info/notice/pages/210522_00.html
https://www.nttdocomo.co.jp/info/spam_mail/column/20190617/

このニュースをザックリ言うと･･･

- 5月22日(日本時間)にNTTドコモより、同27日にはフィッシング対策協議会より、ドコモを騙るSMSによるフィッシング(スミッシング)について注意喚起が出されています。

- フィッシングの例として、「【NTT】お客さまがご利用の電話料金が大変高額になっております。ご確認が必要です」といった文面のSMSで、というドメイン名の偽サイトのリンク先で「NTTセキュリティ」「NTT docomo」を装った不審なスマホアプリのインストール、および「dアカウント」のID・パスワードやネットワーク暗証番号の入力を促すものが挙げられ、不正な決済が発生する事案も確認されているとしています。

- ドコモではこれと前後して商品の発送通知を騙るフィッシングについても取り上げており、「本日商品を発送致しました。詳細は配送状況を で確認ください。」(原文ママ)、「【Amazon】お荷物を出荷致しました、下記よりご確認願います。」という文面例のものが挙げられています。

AUS便りからの所感

- フィッシングの手口は日々様々なものが確認されており、先日は知り合いを騙るSMSを送り付けるスミッシングが発生し(AUS便り 2021/05/25号参照)、また5月28日にはトレンドマイクロより、新型コロナウイルスのワクチン接種予約を騙るスミッシングについて注意喚起が出されています(https://www.is702.jp/news/3864/)。

- 不審なメール・SMSを受信した場合は、フィッシング対策協議会をはじめとするセキュリティ啓発を行っている組織、あるいはドコモをはじめフィッシングにブランドを悪用されている各社からの注意喚起情報、もしくはTwitter等で同様のメール・SMSが報告されていないか確認するとともに、普段利用しているサービスの正規のページへはブラウザーのブックマークに登録してそこからアクセスするよう心掛けましょう。


ITmedia NEWS

ドコモをかたるフィッシングメールやSMSに注意　「dアカウント」のID・パスワードを窃取

2021年05月27日 18時37分 公開　[ITmedia]

印刷　93　Share　B! 1

フィッシング対策協議会は5月27日、NTTドコモをかたるフィッシングメールやSMSを確認したとして注意を呼び掛けた。電話料金や商品発送の案内を偽り、本文中のリンクから偽サイトに誘導するという。

偽メールやSMSの文面