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。

●ソニーミュージックの公式サイト、6日間にわたり公開停止…第三者に改ざんされた形跡

https://www.itmedia.co.jp/news/articles/2004/08/news135.html
https://www.sonymusic.co.jp/page/200405

このニュースをザックリ言うと･･･

- 4月7日(日本時間)、ソニーミュージック社より、同社公式Webサイトを4月1日15時～6日に一時公開停止していたことが発表されました。
- 当該サイトの複数の箇所で第三者による改ざんの形跡が確認されたことが公開停止の理由としています。
- サーバー内の不正な書き込みを削除し、その他の侵入等の形跡もなかったことを確認した上で公開を再開したとしており、サーバー内から個人情報等の漏洩もなかったとしています。

AUS便りからの所感等

- Webサイトの改ざんは現在も世界中で行われており、様々な攻撃者グループが、多数のサイトで同時多発的に改ざんを実行しています。
- 改ざんの内容や意図も単なる愉快犯的なものからマルウェア拡散を意図したものまで様々であり、また今回はメインのWebサイトが被害を受けましたが、既に使用されていない古いサーバーが依然稼動中のところを狙われるケースもあります。
- 組織で使用している全てのサーバー・クライアントの存在を認識・管理し、サーバー側には侵入や改ざんを検知するソリューションを採用し、一方でサーバー管理者のクライアントPC等も踏み台にされないよう、アンチウイルス・UTMにより、入口のみならず出口についても防御を固めて頂ければ幸いです。

SonyMusic

トップ > 「ソニーミュージック オフィシャルサイト」公開停止に関するお詫びと再開のご報告

当サイトの複数のページにおいて、改ざんの形跡が発見されたため、4月1日（水） 15時より一時サイトの公開を停止させていただいておりました。ご利用いただいておりました皆様には、ご迷惑とご心配をおかけしましたことを深くお詫び申し上げます。

全てのページに対して調査を実施するとともに、サーバ内の不正な書き込みを削除し、その他の不正な侵入の形跡もないことが確認されたため、本日4月7日(火)より公開を再開いたしました。
再開まで時間を要することとなってしまい、皆様には、ご不便をおかけしましたことを重ねて深くお詫び申し上げます。

なお、本件によるサーバ内からの個人情報その他の漏洩は確認されておりません。

今後はセキュリティ対策を強化し、皆様が安心してご利用いただけるよう、運営してまいります。

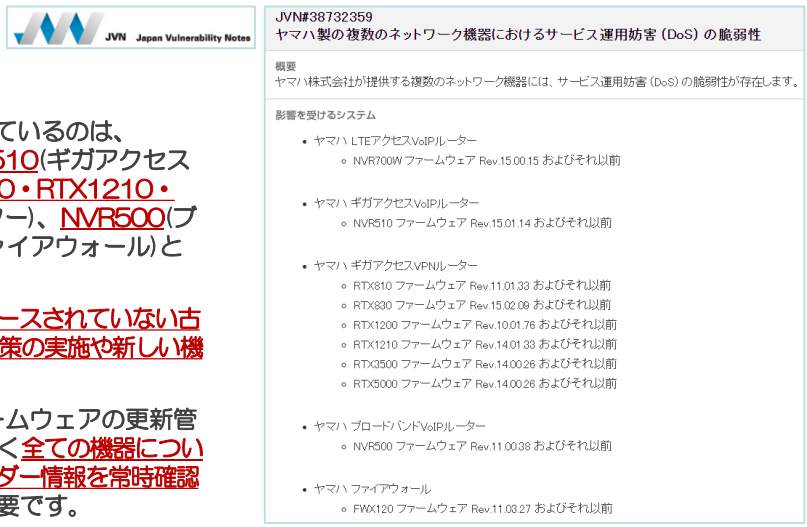
今後とも「ソニーミュージック オフィシャルサイト」をよろしくお願いいたします。

●ヤマハ製ルーター等に脆弱性…ファームウェアのアップデートを

https://news.mynavi.jp/article/20200401-1008414/
https://jvn.jp/jp/JVN38732359/
http://www.rtpro.yamaha.co.jp/RT/FAQ/Security/JVN38732359.html

このニュースをザックリ言うと・・・

- 3月31日(日本時間)、IPAおよびJPCERT/CCより、ルーター等複数のヤマハ製ネットワーク機器にサービス拒否(DoS)攻撃の可能性のある脆弱性が確認されたと発表されました。
- 脆弱性は受信したパケットの処理に起因するもので、攻撃者が不正なパケットを送信した場合に機器が再起動する等の問題が発生するとのことです。
- 同日にヤマハからも詳細が発表され、各種機器においてファームウェアのアップデートが、またアップデートできない場面でも回避策をとることが推奨されています。


JVN Japan Vulnerability Notes

JVN#38732359
ヤマハ製の複数のネットワーク機器におけるサービス運用妨害（DoS）の脆弱性

概要
ヤマハ株式会社が提供する複数のネットワーク機器には、サービス運用妨害（DoS）の脆弱性が存在します。

影響を受けるシステム

- ヤマハ LTEアクセスVoIPルーター
  - NVR700W ファームウェア Rev.15.00.15 およびそれ以前
- ヤマハ ギガアクセスVoIPルーター
  - NVR510 ファームウェア Rev.15.01.14 およびそれ以前
- ヤマハ ギガアクセスVPNルーター
  - RTX810 ファームウェア Rev.11.01.33 およびそれ以前
  - RTX830 ファームウェア Rev.15.02.09 およびそれ以前
  - RTX1200 ファームウェア Rev.10.01.76 およびそれ以前
  - RTX1210 ファームウェア Rev.14.01.33 およびそれ以前
  - RTX3500 ファームウェア Rev.14.00.26 およびそれ以前
  - RTX5000 ファームウェア Rev.14.00.26 およびそれ以前
- ヤマハ ブロードバンドVoIPルーター
  - NVR500 ファームウェア Rev.11.00.38 およびそれ以前
- ヤマハ ファイアウォール
  - FWX120 ファームウェア Rev.11.03.27 およびそれ以前

AUS便りからの所感

- ファームウェアのアップデートがリリースされているのは、NVR700W(LTEアクセスVoIPルーター)、NVR510(ギガアクセスVoIPルーター)、RTX810・RTX830・RTX1200・RTX1210・RTX3500・RTX5000(ギガアクセスVPNルーター)、NVR500(ブロードバンドVoIPルーター)およびFWX120(ファイアウォール)となっています。
- ヤマハでは、上記以外の今回アップデートがリリースされていない古い機種にも脆弱性の影響を受けるとしており、回避策の実施や新しい機種への更新を呼びかけています。
- このようなネットワーク機器はPCに比べファームウェアの更新管理が疎かにされがちな傾向がありますが、とにかく全ての機器についてファームウェアバージョン情報を把握、またベンダー情報を常時確認し、確実に対策を実施できる体制を整えることが重要です。

●iPhoneに突然表示される、不審なカレンダー通知…IPAが注意喚起

https://www.itmedia.co.jp/news/articles/2003/30/news139.html
https://www.ipa.go.jp/security/anshin/mgdayori20200330.html

このニュースをザックリ言うと・・・

- 3月30日(日本時間)、IPAの「安心相談窓口だより」において、今年1月から3月にかけて、iPhoneのカレンダー機能に関する相談が複数件寄せられたとして注意喚起が出されています。
- 相談の内容は「iPhoneのカレンダーから、ウイルス感染しているという通知が出る」「iPhoneのカレンダーに、身に覚えのないイベントが入っている」といったもので、イベントのタイトルは「ウイルスに感染している可能性があります」「あなたのiPhoneは保護されていません！」、また併記されているURLのタップにより、不審なサイトへ誘導される恐れがあるとしています。
- IPAでは、身に覚えのない共有カレンダーへの参加依頼が来た場合、イベントの予定を削除しスパム報告をすること、また記載されているURLをタップしないことを呼びかけています。

AUS便りからの所感

- IPAの解説によれば、これはiCloudカレンダーの「共有機能」「出席以来機能」を悪用した手口で、攻撃者は何らかの方法で相手のiCloudメールアドレスを知った上でそのアドレスを共有先として設定することにより、不審なカレンダーやイベントを登録しているとのことです。
- iPhoneのカレンダー機能の正規の機能を悪用したものであり、Appleがこれに対し何らかの対策を行うかは不明ですが、見ず知らずの相手が事前の連絡なしにカレンダーやオンラインストレージ等の共有サービスへの参加を依頼してきた場合に安易に承諾しないことは、以後の様々な不審な行為を遮断する意味で十分に意識すべき対応と言えるでしょう。


IPA

iPhoneに突然表示される不審なカレンダー通知に注意！

一覧を見る

今年1月から3月にかけて、「iPhoneのカレンダーから、ウイルス感染しているという通知が出る」、「iPhoneのカレンダーに、身に覚えのないイベントが入っている」といった相談が複数件寄せられました。

これは、iCloudカレンダーの機能を悪用して、他人のカレンダーに不審な書き込みを行う手口です。

図1：不審なカレンダー通知の手口イメージ

ここでは、手口および対処、被害にあわないための対策について解説します。