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。

●QNAP社製NASに感染、マイニングを行うマルウェア確認…パッチ未適用のNASに注意喚起

https://pc.watch.impress.co.jp/docs/news/1310879.html
https://blog.netlab.360.com/qnap-nas-users-make-sure-you-check-your-system/
https://www.qnap.com/en-us/security-advisory/qsa-20-08

このニュースをザックリ言うと･･･

- 3月5日(現地時間)、中国のセキュリティ企業Qihoo 360(奇虎360)より、QNAP社製NASの脆弱性を突いて感染するマルウェアについて注意喚起が出されています。
- 注意喚起によれば、このマルウェアは、外部から不正なコマンドを実行可能な脆弱性(CVE-2020-2506・CVE-2020-2507)により、NAS上で仮想通貨のマイニングを行うプログラムを設置するとされています。
- 脆弱性自体は2020年10月リリースのファームウェアで対策されていますが、全世界で数十万台のQNAP社製NASがアップデートを行っておらず、攻撃を受ける可能性があるとされています。

AUS便りからの所感等

- 脆弱性が存在するのはNAS専用OS「QTS」に含まれる「Helpdesk」アプリケーションで、バージョン3.0.3へのアップデートにより、対策されるとのことです。
- 日本においてはNATにより外部から直接アクセスできないネットワーク構成となっているケースが一般的でしょうが、いわゆる「プライベートクラウド」の構築のために外部の任意のアドレスからNASのWebインタフェースにアクセス可能な設定となっている場合、ユーザー以外の第三者、即ち攻撃者もアクセスする恐れがあるものと注意する必要があります。
- ユーザーが普段利用するクライアントPCのみならず、サーバーやネットワーク機器においても、ファームウェア等のアップデートを確実に行う設定、そして確認する体制を整えることが肝要です。

Impress Watch

パッチ適用前のQNAP NASで密かにマイニングするマルウェアが蔓延

劉 尭　2021年3月9日 15:23

Network Security Research Lab at 360は5日、セキュリティパッチ適用前のQNAP製NASを標的とし、脆弱性を悪用して密かにマイニングをするマルウェアの攻撃について報告、ユーザーに警鐘を鳴らした。

このマルウェアは、リモートで不正なコマンドを実行できる脆弱性(CVE-2020-2506、およびCVE-2020-2507)を利用し、デバイスに入っているオリジナルのmanaRequest.cgiをハイジャック。その後マイニングプログラムをセットアップ、実行する。

QNAP

Resolved Multiple Vulnerabilities in Helpdesk

Release date: October 7, 2020
Security ID: QSA-20-08
Severity: Critical
CVE identifier: CVE-2020-2506 | CVE-2020-2507
Affected products: Helpdesk
Status: Resolved

Summary
Two vulnerabilities have been reported to affect earlier versions of QTS.

- **CVE-2020-2506:** If exploited, this improper access control vulnerability could allow attackers to gain privileges, or read sensitive information.
- **CVE-2020-2507:**If exploited, this command injection vulnerability could allow remote attackers to run arbitrary commands.

QNAP has already fixed these issues in Helpdesk 3.0.3 and later versions.

Recommendation
To fix the vulnerability, we strongly recommend updating Helpdesk to the latest version.

● Windowsの月例アップデートで不具合報告相次ぐ…一部メーカー複合機での印刷でブルースクリーン発生

https://pc.watch.impress.co.jp/docs/news/1311595.html
https://pc.watch.impress.co.jp/docs/news/1311951.html
https://docs.microsoft.com/en-us/windows/release-health/status-windows-10-20h2#1570msgdesc

このニュースをザックリ言うと･･･

- 3月10日(日本時間)にマイクロソフト(以下・MS)よりリリースされた月例のセキュリティパッチを適用したWindows10等で不具合が相次いで報告される事態となっています。

- 不具合が報告されているのは、Windows 10 2004/20H2向けパッチ「KB5000802」および同1909向けパッチ「KB5000808」等(以下・当該パッチ)で、適用後にリコーや京セラ等の一部メーカー製複合機での印刷時にブルースクリーンが発生すると報告されています。

- MSでは不具合について調査を進め、進捗があり次第情報を更新するとし、回避策も提示しています。

AUS便りからの所感

- 当該パッチによる不具合としては、他にも詳細不明ながら、Excel実行時やFAX送信時にもブルースクリーンが発生するという事象も報告されている模様です。

- 画面左下(デフォルト)のWindowsアイコンクリック→「設定」→「更新とセキュリティ」→「更新の履歴を表示する」→「更新プログラムをアンインストールする」から当該パッチのアンインストールを行うことでも回避可能ですが、同じパッチが再度インストールされないよう「更新を7日間一時停止」し、また事象が解決された新しいパッチがリリースされた場合は「更新の再開」を行う必要があります。

- そしてその間は、当該パッチに含まれていたセキュリティ修正も適用されない状態であることには注意しなければならず、このような事態において脆弱性の根本的な対策が行われていない状態の各PCが攻撃を受ける可能性を少しでも抑制するためには、普段からアンチウイルスやUTM等による防御を固めておくことが必要不可欠です。

- (3/16追記)不具合を修正したとする新しいパッチ「KB5001567」「KB5001566」がリリースされています。

Impress Watch

Windows 10の印刷時ブルースクリーン問題。Microsoftが回避策公開

中村 真司　2021年3月15日 06:10

米Microsoftは、Windows 10でプリント時にブルースクリーンが発生するという問題に関して、回避策を公開した。

この問題はWindows 10の累積アップデート「KB5000802」を適用したPCにて発生しており、特定のプリンタで印刷すると「APC_INDEX_MISMATCH」というエラーメッセージが出るとともに、ブルースクリーンが表示されてしまうというもの。

原因はType 3のプリンタドライバにあり、その改良版であるType 4のプリンタドライバでは発生しないとする。自分のプリンタがどちらのドライバを使っているかは、「印刷の管理」からプリントサーバーのツリーを展開すれば確認できる。

● 「コンピュータが危険」ブラウザ通知から不審サイトに誘導… IPA「安易に通知許可しないで」

https://www.itmedia.co.jp/news/articles/2103/12/news110.html
https://www.ipa.go.jp/security/anshin/mgdayori20210309.html

このニュースをザックリ言うと･･･

- 3月9日(日本時間)、IPAの「安心相談窓口だより」において、PCおよびAndroid端末におけるWebブラウザーの通知機能を悪用して不審なサイトに誘導しようとする攻撃について取り上げられています。

- 手口の例として、サーチエンジン等からアクセスしたサイトにおいて「ロボットでない場合は、[許可]をクリックします」等と表示して通知の許可を行うよう誘導→許可したサイトから「お使いのPCがマルウェアに感染しています」といった虚偽の警告が通知→その通知をクリックすることにより、偽のセキュリティソフト購入サイト、偽のキャンペーン当選サイト、あるいは不審なAndroidアプリをインストールさせようとするサイト等に誘導される、というものが挙げられており、大手セキュリティベンダーを騙るものも存在する模様です。

- IPAでは「安易に通知を許可しない」「表示された通知表示に注意する」「通知表示から誘導されたサイトで操作しない」よう呼び掛けており、PC・Androidの各種ブラウザーから誤って登録した通知許可を削除する方法等も紹介しています。

AUS便りからの所感

- 偽の警告をブラウザーやPCの画面上に表示して脅しをかける手口は「スケアウェア」と呼ばれ、2000年代から存在しています。

- 手口の最初の段階である「通知の許可を求める」サイトは、Google等で複数の日本語キーワードで検索しても辿り着く可能性もあり、多くは「許可しないと先に進めない」ように見せかけていますが、全て同様の手口であると考え、決して許可しないようにしましょう(信頼できる有名なサイトであっても、リアルタイムで新着記事を見たいというものでない限りはブロックする方針をとるのが、いざというときに安全です)。

- 特にAndroidにおいては、アプリのインストールによりスマートフォン上のあらゆる情報へのアクセスを許可しかねず、インストール時等に不自然に様々な権限を要求してくるものには注意を払いましょう。

ITmedia NEWS

「コンピュータが危険」ブラウザ通知から不審サイトに誘導　IPA「安易に通知許可しないで」

2021年03月12日 14時53分 公開　[ITmedia]

印刷　見る　Share　B! 30

PCやAndroidスマートフォンのWebブラウザ利用中に「コンピュータが危険にさらされている」などの偽メッセージが繰り返し表示され、不審なサイトに誘導された――このような相談が寄せられているとして、情報処理推進機構（IPA）は「安易に通知を許可しないで」と注意を呼び掛けている。

通知機能はiOSにはないため、偽のメッセージが表示される可能性があるのはPCとAndroid端末のみ。