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。

●Windowsの印刷サービスにゼロデイ脆弱性「PrintNightmare」、MSはサービス停止推奨

https://forest.watch.impress.co.jp/docs/news/1335872.html
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-34527
https://www.ipa.go.jp/at/2021/at210029.html

このニュースをザックリ言うと・・・

- 6月29日（現地時間）、Githubにおいて、Windowsの印刷スプーラー（Print Spooler）に存在する脆弱性「PrintNightmare」に関する情報および実証コードが公開されました（間もなくGithubからは削除されたものの、内容は既に広まっている模様です）。

- 印刷スプーラーにアクセス可能な攻撃者が、これが動作しているサーバーを乗っ取ることが可能になるとされ、7月1日にマイクロソフト（以下・MS）より、まだ修正パッチがリリースされていない、いわゆる「ゼロデイ脆弱性」として正式に発表されています。

- MSでは、6月の月例パッチで修正された印刷スプーラーの脆弱性（CVE-2021-1675）とは別の脆弱性であるとし（新たなCVEとして「CVE-2021-34527」が割当てられています）、パッチがリリースされるまでの回避策として、Print Spoolerサービスを無効にすること等を推奨しています（ただしこれにより、印刷が実行できなくなります）。

AUS便りからの所感等

- PrintNightmareは当初、6月に修正されたCVE-2021-1675と同一のものとされ、一旦は対策済みと判断して公開されたものの、未修正の別の脆弱性であることが判明し、結果としてゼロデイの脆弱性となったことが、Githubからコンテンツが取り下げられた理由とみられています。

- 印刷スプーラーにおいては2020年5月にも、四半世紀の間存在していたとされる脆弱性「PrintDemon（CVE-2020-1048）」が報告・修正される等、以前から脆弱性が度々報告されており、印刷を行う予定のないPCや、プリントサーバーでないWindowsサーバー、特にActive Directory環境におけるドメインコントローラについては、サービス管理画面等から（MSの情報ではPowerShellスクリプトによる方法も紹介されています）印刷スプーラーサービスを停止・無効化するといった回避策をとることを強く推奨致します。

- Windowsではサーバーのみならずクライアントでも数多くのサービスが稼働しており、根本的な対策として修正プログラムを速やかに適用する体制はもちろん、攻撃の余地を与えないよう可能な限り不要なサービスを停止するとともに、OS自体のファイアウォール機能ないしアンチウイルス・UTM含め各種ソリューションによる防御を徹底することが肝要です。

Impress Watch

Microsoft、「PrintNightmare」脆弱性の緩和策を公表 ～「CVE-2021-34527」が新たに割り当てられる

6月にパッチされた問題「CVE-2021-1675」とは別。攻撃手法がすでに出回っており、警戒が必要

樽井 秀人　2021年7月5日 10:00

同社のサポートドキュメント

米Microsoftは7月1日（現地時間）、Windows印刷スプーラーで任意コードの実行が可能になるゼロデイ脆弱性「PrintNightmare」に対する緩和策を発表した。この脆弱性には「CVE-2021-34527」という識別番号が新たに割り当てられている。

「PrintNightmare」は、先日「GitHub」で公表されたWindows印刷スプーラーの脆弱性を突いた攻撃手法。システム特権で任意のコードが実行される可能性があり、具体的なコードも知られているが、まだ対策されていない。

●2010年出荷のWD製NASに脆弱性、リモートからの攻撃でデータ消失の恐れ…ネットからの切断推奨も

https://pc.watch.impress.co.jp/docs/news/1334478.html
https://gigazine.net/news/20210630-wd-my-book-live-exploited-0-day/

このニュースをザックリ言うと･･･

- 6月25日(現地時間)、HDD・SSD等製造大手の米Western Digital社(以下・WD)より、同社が出荷した古いNASに存在する未修正の「ゼロデイ脆弱性」を悪用する事例が多発しているとして注意喚起が出されています。

- 対象となるのは2010年に出荷されたNAS「My Book Live」「My Book Live Duo」で、NAS上で任意のコマンドを実行する脆弱性(CVE-2018-18472)を悪用し、NASの初期化・データの抹消を行う攻撃が同24日から相次いでWD社の公式フォーラムに報告されているとのことです。

- 当該NASのサポートは2015年で終了しており、WD社では回避策として、これらの製品をネットワークから切断することも呼び掛けています。

- なお、WD社が現在販売する「My Cloud OS 5」および「My Cloud Home」を使用している他の製品は脆弱性の影響を受けないとしています。

AUS便りからの所感

- 攻撃を受けたというNASはUPnPによって外部から接続できるよう自動的に設定されていた模様で、「リモートアクセス」機能がデフォルトで有効になっていた(https://internet.watch.impress.co.jp/docs/column/shimizu/549646.html)ために、攻撃者にターゲットとして検索されたと推測されます。

- ブロードバンドルーター側で指定したサーバーのみアクセスするようポートの設定を行ったとしても、内部にUPnPを利用するサーバー等を設置することにより、そのサーバーも外部からアクセス可能となる可能性がありますので、ルーター側・サーバー側双方でUPnPの設定を確認し、意図しないサーバーの公開が行われないよう、必要に応じUPnPを停止する等の対策をとることが重要です。

- 今回のケースを鑑みれば、前述のとおり問題となったNASのサポートは既に終了しており、また脆弱性もその後になって発見された模様ですので、脆弱性の修正が見込めない古い機器を速やかに新しい機器に交換できる体制を是非とも整えるようにしてください。

Impress Watch

WD製NASに脆弱性、今すぐネット切断を。フルリセットで全データ消失

劉 尭　2021年6月28日 15:25

米Western Digital(WD)は25日(現地時間)、同社が2010年に出荷したNAS「My Book Live」および「My Book Live Duo」に脆弱性があるとし、現在も使用しているユーザーはすぐにネットから切断するよう注意を促した。

脆弱性の詳細はまだ解析中としているが、報告があったデバイスのログを確認すると、UPnPを使って自動的、もしくは手動でポートフォワードされたポートを経由し、複数の国のIPアドレスから直接本体にアクセスした形跡があった。そのため、攻撃者はポートスキャンを通して脆弱性を発見したと見ている。

●オリコン社員メールアカウントに不正アクセス…取引先17,625人分の情報流出か

https://www.itmedia.co.jp/news/articles/2106/30/news146.html

このニュースをザックリ言うと･･･

- 6月30日(日本時間)、オリコン社より、同社社員のメールアカウント1件が外部からの不正ログインを受けたことが発表されました。

- 不正ログインにより、メールボックス上のメールにアクセスされ、ビジネス上の取引先17,625名の個人情報(氏名・勤務先のメールアドレス・会社・部署・住所・電話番号)等が読み取られた可能性があるとしています(金融口座・クレジットカード等の情報は含まれないとのことです)。

- 同16日、取引先より、当該取引先とオリコン社とのやり取りメールが引用された形で外部メールアドレスから不審なメールが送信されたとの連絡があり、不正ログインが発覚したとのことです。

- メールサーバーの脆弱性を突いての外部からの不正アクセスにより、メールアカウントのパスワードが奪取されたことが原因としています。

AUS便りからの所感

- オリコン社では当該アカウントを含め全従業員のパスワードの再設定を行った他、承認された特定のデバイスからのみメールシステムにアクセス可能とする設定を行ったとしています。

- 特定のメールアカウントが不正ログインを受け、SPAMメールの大量送信に悪用されるケースや、今回のようにメールボックスを読み取られるケースはこれまでも度々あり、侵入経路についても脆弱なパスワードの推測からPCに感染したマルウェアまで様々ですので、前述のようなデバイスの限定や二要素認証等によるメールアカウントへのアクセス制限を検討すること(従来のメールシステムでそういった設定ができなければ、メールシステムの刷新も考慮することになるでしょう)、方やPCがマルウェアに感染しないようアンチウイルスやUTMによる防御等、各種対策をとっていくことを推奨致します。

ITmedia NEWS

オリコン、取引先情報1万7000件漏えいの可能性　社員のメールアカウントに不正ログイン

2021年06月30日 16時36分 公開　[吉川大貴，ITmedia]

オリコンは6月30日、社員1人のメールアカウントが不正ログインされ、1万7625人分の取引先情報が漏えいした可能性があると発表した。メールサーバのセキュリティホールを突いた不正アクセスでパスワードを窃取されたという。

漏えいした可能性があるのは、該当の社員とメールをやりとりしたことがある人の氏名、メールアドレス、会社名、部署名、勤務先の住所や電話番号など。口座情報やクレジットカード情報などは含まれていないという。メッセージの内容を抜き取られ、迷惑メールに利用された例も1件確認した。