NTT DATA
Trusted Global Innovator

注目されているセキュリティ事故・事件に関する情報 ＜2019年12月版 (第31号)＞(選り抜き版)

2019年12月25日
ＮＴＴデータ先端技術株式会社
セキュリティ事業本部

© 2021 NTT DATA INTELLILINK Corporation

今回のサマリー

VPN製品の脆弱性を悪用した攻撃に注意

2019年9月、JPCERT/CCから、複数のインターネットVPN製品について、リモートコード実行や認証情報の窃取が可能となる脆弱性を悪用した攻撃の注意喚起が行われました。その中でも、Pulse Secure社のVPN製品については、8月以降、実際にその脆弱性が悪用されたと考えられる事例が発生しています。

本記事では、 Pulse Secure社のVPN製品に焦点を当て、脆弱性や攻撃フロー、事例、企業が取るべき対策について解説します。

© 2021 NTT DATA INTELLILINK Corporation

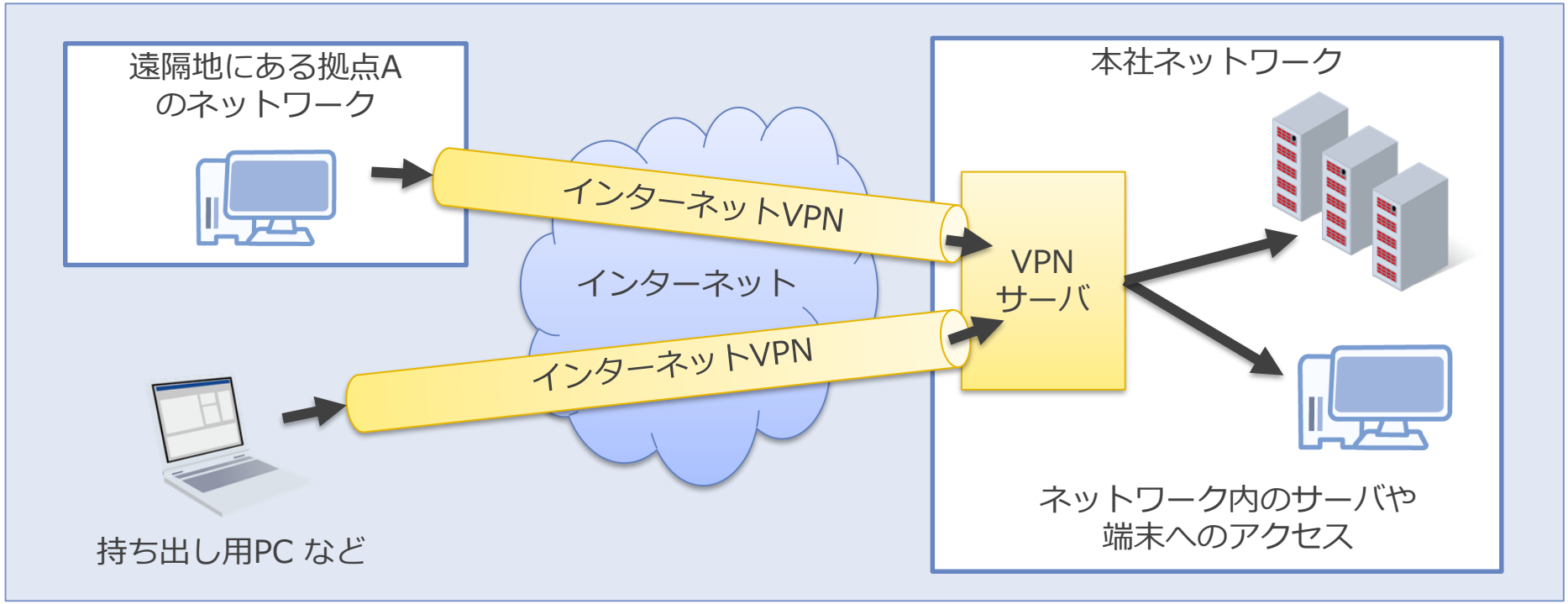
VPN製品の脆弱性を悪用した攻撃に注意

© 2021 NTT DATA INTELLILINK Corporation

1. インターネットVPNとは

インターネットVPN(Virtual Private Network)とは、インターネット上で、クライアントとサーバ間で暗号化された通信経路を作る仕組みです。企業においては、インターネットを経由した拠点間の接続や、外部のクライアントから企業内のネットワークへ接続する際に用いられます。

このようなインターネットVPNの商用製品は、Pulse Secure社、Palo Alto Networks社、Fortinet社など、複数ベンダが提供しています。

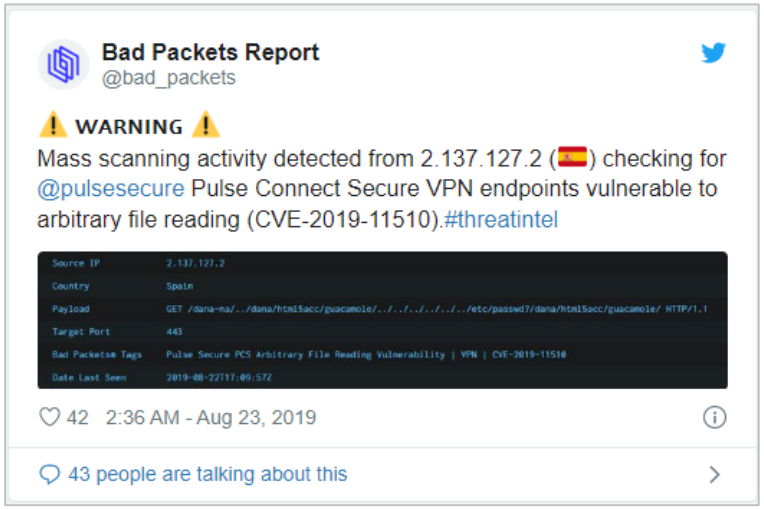


インターネットVPNの利用イメージ

2. インターネットVPN製品を狙った攻撃

2019年9月に、JPCERT/CCより、複数のインターネットVPN製品について、認証情報の窃取などが可能な脆弱性を悪用した攻撃が観測されていると報告されました。特に、Pulse Secure社のVPN製品(以降、Pulse Secure VPN)については、8月から継続的に、脆弱性の探索とみられる通信が多数観測されている旨がTwitter上でも報告されており、実際にその脆弱性が悪用されたと考えられる事例も発生しています。

JPCERT/CC：複数の SSL VPN 製品の脆弱性に関する注意喚起
https://www.jpcert.or.jp/at/2019/at190033.html



OVER 14,500 PULSE SECURE VPN ENDPOINTS VULNERABLE TO CVE-2019-11510
https://BadPackets.net/over-14500-pulse-secure-vpn-endpoints-vulnerable-to-cve-2019-11510/

本記事では、Pulse Secure VPNに焦点を当て、脆弱性や攻撃フローについて説明します。

3. Pulse Secure VPNの脆弱性の詳細

2019年4月に、Pulse Secure社より、Pulse Secure VPNに関する複数の脆弱性の情報が公開されました。脆弱性の中でも、「CVE-2019-11510」が攻撃者に悪用されると、VPNサーバに保存された認証情報が平文のまま窃取され、VPNサーバに不正ログインされるなどのリスクがあります。

CVE番号	脆弱性の内容	影響を受ける製品/バージョン
CVE-2019-11510	認証前の任意のファイル読取	【Pulse Connect Secure】 • 9.0R1 - 9.0R3.3 • 8.3R1 - 8.3R7 • 8.2R1 - 8.2R12 • 8.1R1 - 8.1R15 【Pulse Policy Secure】 • 9.0R1 - 9.0R3.1 • 5.4R1 - 5.4R7 • 5.3R1 - 5.3R12 • 5.2R1 - 5.2R12 • 5.1R1 - 5.1R15 ※物理アプライアンス/仮想アプライアンスともに、影響を受けます。
CVE-2019-11542	認証後(管理者権限)のスタックバッファオーバーフロー	
CVE-2019-11539	認証後(管理者権限)のコマンドインジェクション	
CVE-2019-11538	認証後(ユーザ権限)のNFS経由の任意のファイル読取	
CVE-2019-11508	認証後(ユーザ権限)のNFS経由の任意のファイル書込	
CVE-2019-11540	認証後のクロスサイトスクリプトインクルージョン	
CVE-2019-11507	認証後クロスサイトスクリプティング	

© 2021 NTT DATA INTELLILINK Corporation

4. Pulse Secure VPNの脆弱性に関する動向

2019年4月に、Pulse Secure VPNの脆弱性が公開された後に、セキュリティ関連の研究者や企業などから、相次いでVPNサーバに関する攻撃事例や注意喚起が発表されました。また、Pulse Secure VPNの脆弱性の悪用事例も報告されています。

年月	内容
2019年4月	Pulse Secure社より脆弱性が公開される。
2019年5月	5月28日に、研究者のOrange Tsai氏が、Pulse Secure VPNの脆弱性を使用してTwitter社のネットワークへの侵入に成功した。この件はバグバウンティプログラム「HackerOne」で報告され、現在は修正されている。
2019年8月	GithubでPoC (※) が公開される。
	脆弱性の探索活動が行われていることが、Twitterの @bad_packets により報告される。
2019年9月	JPCERT/CCから注意喚起が行われる。(複数の SSL VPN 製品の脆弱性に関する注意喚起)
2019年10月	情報セキュリティの国際会議「CODE BLUE」にて、脆弱性を悪用した攻撃事例が紹介される。
	10月25日に、三菱UFJ銀行は、VPNサーバに対する不正アクセスにより、台湾拠点の取引先や従業員等の第三者に関する情報 計1,305 の情報漏えいがあったと報告した。具体的なVPN装置は公式発表されていないが、有識者により、Pulse Secure VPNであった可能性が高いとされている。
2019年11月	11月5日に、Twitterの @bad_packets により、セブンイレブンが脆弱性があるPulse Secure VPNを使用していると報告される。

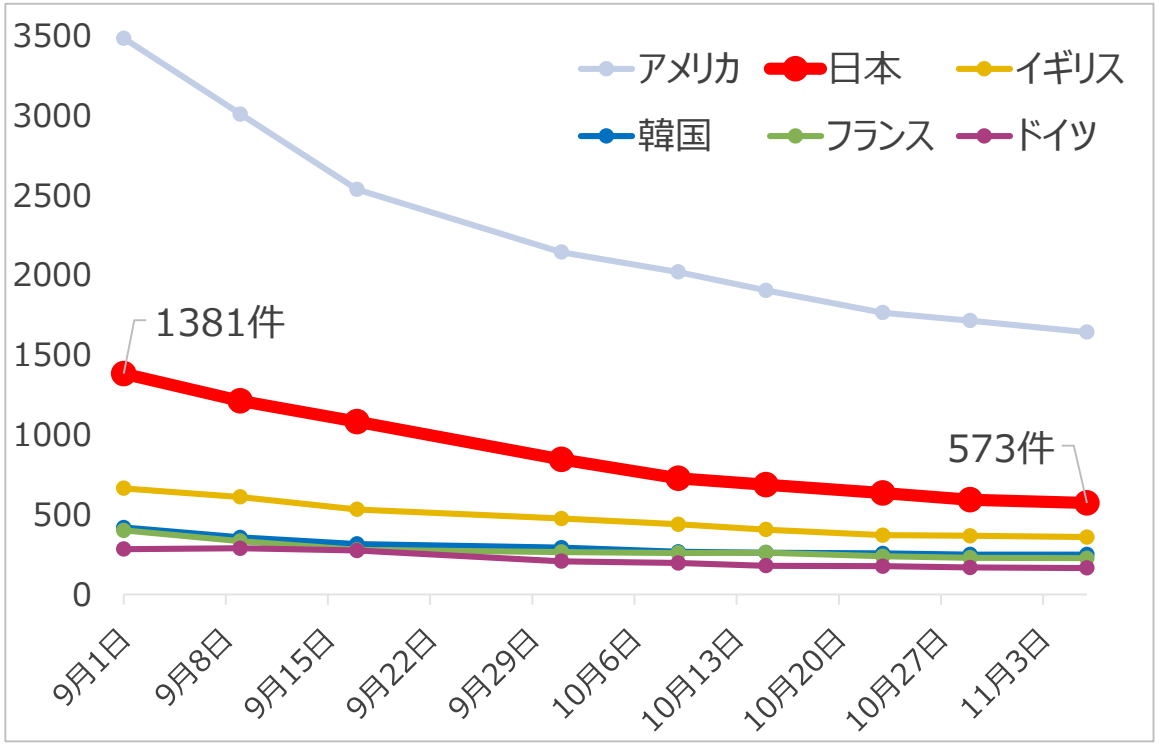
※ PoC (Proof of Concept): 概念実証の意味。セキュリティの分野では、脆弱性を悪用した攻撃が実際に可能であるかを検証するためのプログラムのことを指す。「Exploitコード」と呼ばれることもある。

© 2021 NTT DATA INTELLILINK Corporation

5. 未対策となっているPulse Secure VPNの数

Bad Packetsによる調査では、日本国内の脆弱性がある(アップデートしていない)Pulse Secure VPNの数が、世界で2番目に多いとされています。
各国ともに、アップデートにより脆弱性がある機器の数は減少傾向にありますが、減少量(アップデートの進み具合)は日ごとに横ばいになりつつあります。

2019年11月5日 14:08 の @bad_packets によるツイート
https://twitter.com/bad_packets/status/1191839806432526337



@bad_packets による調査結果をグラフ化したもの
(縦軸は 未対策のPulse Secure VPNの数)

6. Pulse Secure VPNの脆弱性による影響

Pulse Secure VPNの脆弱性を悪用された場合、以下の影響を受ける可能性があります。

【初期の攻撃】

- VPNサーバの認証情報の窃取

窃取した認証情報で、VPNサーバへの不正ログインに成功した場合

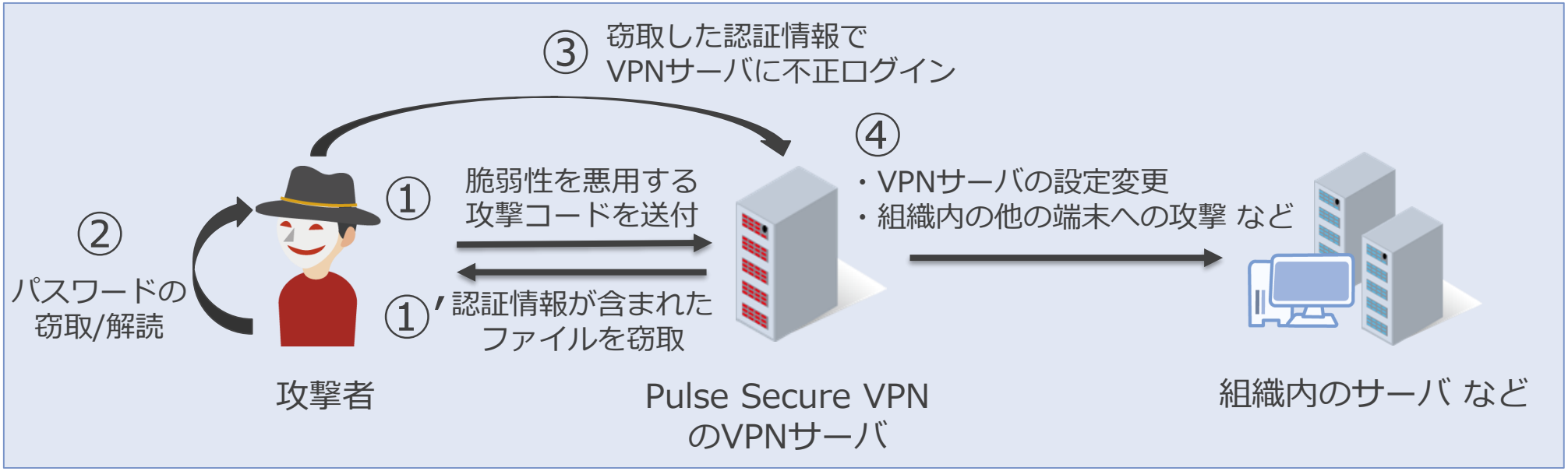
【窃取した認証情報による不正ログイン後】

- VPNサーバの設定値の変更
- 企業のネットワークへの不正侵入
- 企業のネットワークに接続されている他のサーバへの攻撃
- VPNで接続してきた端末への攻撃

© 2021 NTT DATA INTELLILINK Corporation

7. Pulse Secure VPN 攻撃フローの概要

Pulse Secure VPNの脆弱性を悪用した攻撃は、以下の通り行われます。



① インターネット上に公開されているPulse Secure VPNのVPNサーバに対して、CVE-2019-11510を悪用して、以下のファイルを取得する。
　★ /data/runtime/mtmp/lmdb/dataa/data.mdb
　☆ /data/runtime/mtmp/system

② 上記のファイルのうち、★のファイルから、平文で保存された認証情報を抽出する。認証情報を見つけることができない場合は、攻撃者は☆のファイルにあるハッシュ化されたパスワードのリストを収集し、 ハッシュを解読する。

③ ②で窃取した認証情報で、VPNサーバに不正ログインする。

④ VPNサーバの設定の変更や、VPNサーバ上での任意のコマンド実行などにより、他の端末への攻撃を試みる。

© 2021 NTT DATA INTELLILINK Corporation

8. Pulse Secure VPNの攻撃への対策

Pulse Secure社によると、アップデート以外に脆弱性の修正方法はないとしています。影響を受ける製品とバージョンを確認し、修正済みバージョンへのアップデートをお勧めします。

影響を受ける製品	影響を受けるバージョン	修正済みバージョン
Pulse Connect Secure	9.0R1 - 9.0R3.3	9.0R3.4 & 9.0R4
	8.3R1 - 8.3R7	8.3R7.1
	8.2R1 - 8.2R12	8.2R12.1
	8.1R1 - 8.1R15	8.1R15.1
Pulse Policy Secure	9.0R1 - 9.0R3.1	9.0R3.2 & 9.0R4
	5.4R1 - 5.4R7	5.4R7.1
	5.3R1 - 5.3R12	5.3R12.1
	5.2R1 - 5.2R12	5.2R12.1
	5.1R1 - 5.1R15	5.1R15.1

© 2021 NTT DATA INTELLILINK Corporation

9. アップデート意識の薄れの問題

ここまで、Pulse Secure VPNを例に、事例から対策までを紹介しました。しかし、今回のVPN製品に限らず、ルータなどのインターネットに公開された機器の脆弱性が悪用される事例は、過去にも多数報告されています。

時期	事例概要	詳細	
2017年12月	Mirai 亜種の感染	対象機器	ロジテック社製のブロードバンドルーター
		被害機器数	最大2万4000台
		参考URL	https://www.jpcert.or.jp/at/2017/at170049.html https://internet.watch.impress.co.jp/docs/news/1097777.html
2018年5月	VPN Filterの感染	対象機器	QNAP / Linksys / MikroTik / NETGEAR / TP-Link 社製のネットワーク機器、NAS
		被害機器数	少なくとも、50万台
		参考URL	https://blog.talosintelligence.com/2018/05/VPNFilter.html https://www.jpcert.or.jp/newsflash/2018052401.html

一般的に、脆弱性への対策は「アップデート」が有効です。ただしネットワーク機器のような、ユーザが直接操作する機会が少ない機器については、OSやアプリケーションと比較して、「脆弱性が存在し、アップデートが必要であるという意識」が低くなりがちです。これにより、上記のような悪用事例が相次いでいると考えられます。

© 2021 NTT DATA INTELLILINK Corporation

10. 脆弱性への全般的な対策 (1/3)

アップデートの意識を高めるためには、「アップデートする」ことを運用業務の中に確実に含めることが必要です。また、アップデートのための費用や稼働の確保、機器の一覧化、脆弱性の情報収集も必要になります。

■ **運用計画の策定**

機器によっては、保守契約を結ばない場合、アップデートができないことも考えられます。また、以降に示す活動を行う上で、人的リソースも必要になります。機器の導入前に、予算や稼働の確保を含めた運用計画を立てることが必要です。

■ **資産管理**

特に、ネットワークやサーバなどのインフラで使用されている機器については、運用者やユーザが日常的に操作するものではないため、その存在を意識することが少なくなります。以下に示す対応を定期的に行い、機器やバージョンを明らかにしておくことが大切です。

- 企業内で使用している機器を定期的に洗い出す
  ⇒特に、インターネットに公開している機器は攻撃を受ける可能性が高いため、必ず実施する
- 機器のバージョン情報を最新化する
- 保守契約の締結状況やその期限を一覧化する

© 2021 NTT DATA INTELLILINK Corporation

10. 脆弱性への全般的な対策 (2/3)

■ **脆弱性/アップデート情報の収集**

前述の「■資産管理」で一覧化した機器とバージョンの情報をもとに、脆弱性の情報を検索しアップデートの有無を確認します。脆弱性情報の収集先や収集方法には、以下があります。

情報収集先の例	収集方法
• ベンダの公式Webサイト • JVNやNVD上の情報 • JPCERT/CCやIPAからの注意喚起情報 • ニュースサイトの情報 など	• [運用的] 運用者による定期的な情報収集 • [システム的] ベンダからのメール • [システム的] 脆弱性情報配信サービスの利用 • [システム的] RSS等を利用した脆弱性情報の通知 など
参考: 脆弱性対策の効果的な進め方 ツール活用編 https://www.ipa.go.jp/topic/isec-technicalwatch-201902.html	

脆弱性管理の対象となる機器が多数ある場合、収集すべき脆弱性の情報も多くなり、管理が難しくなる場合があります。この場合は、脆弱性管理システム (※) の導入もご検討ください。

※ 商用製品として、Tenable社の「Tenable.io」や、Qualys社の「QualysGuard」などがあります。

© 2021 NTT DATA INTELLILINK Corporation

10. 脆弱性への全般的な対策 (3/3)

■ **アップデート**

前述の「■資産管理」や「■脆弱性/アップデート情報の収集」の結果をもとに、アップデート対象となる機器について、アップデートを行います。

特に、ネットワーク機器やアプライアンス製品は、アプリケーションやOS等と比較して、「脆弱性の存在意識」や「アップデートの意識」が低くなりがちです。これらの機器/製品にも脆弱性が存在し、アップデートが必要であることを認識することが大切です。

アップデートは、機器のインターネットへの公開有無に関わらず実施することが大切です。インターネットに公開していない機器もアップデートすることで、仮に他の方法で企業内のネットワークに侵入された場合でも、踏み台などに使われる被害を最小限にすることができます。

なお、アップデートによる業務停止などのリスクを考慮する場合は、検証用の環境等で十分な検証した上で、業務への影響がないかを確認することをお勧めします。

© 2021 NTT DATA INTELLILINK Corporation

11. その他の対策

■ **低減策**

以下に示す対策は、脆弱性の根本的な対策ではありませんが、攻撃を受ける可能性を少なくすることができます。

- アクセス制御
  ⇒アクセス可能な送信元IPアドレスを制限することにより、攻撃を受ける可能性を低減させることが可能です。

■ **攻撃を受けた後の備え**

攻撃を受けた場合を想定して、以下の対策も行うことをお勧めします。

- ログの取得/監査
  ⇒不正ログインなどのインシデントの発生を素早く検知したり、原因解明や被害範囲などの調査を行いやすくするために、ログを取得する設定となっているかを確認します。また、意図しないアクセスや設定変更がないことを定期的に確認します。

© 2021 NTT DATA INTELLILINK Corporation

12. まとめ

本記事では、「Pulse Secure VPN」に焦点を当て、脆弱性や攻撃フロー、事例、企業が取るべき対策について解説しました。

VPNのように、業務をセキュアに行うために導入した製品/機器であっても、適切に管理を行っていない場合、その製品/機器が弱点となり、攻撃者に狙われる対象となります。実際に、2019年8月以降、複数のVPN製品で脆弱性を悪用した攻撃がインターネット上で確認されており、その脆弱性が悪用されたと考えられる事例も発生しました。

通常は脆弱性対応としてアップデートを行いますが、ネットワーク機器やアプライアンス製品などの場合は特に「脆弱性が存在し、アップデートが必要であるという意識」が低くなりがちです。これにより、脆弱性対応が済んでいない機器が増え、悪用事例が相次いでいると考えられます。

機器/製品の導入の際は、アップデートのための予算や稼働を考慮した運用計画を検討することが大切です。その上で、日々の運用業務として、「資産管理」や「脆弱性情報の収集」、「アップデート」のサイクルを継続的に行う必要があります。アップデートの意識が低くなりやすいネットワーク機器やアプライアンス製品なども確実に確認・実施することが重要です。

© 2021 NTT DATA INTELLILINK Corporation

13. 参考URL

- Public KB - SA44101 - 2019-04: Out-of-Cycle Advisory: Multiple vulnerabilities resolved in Pulse Connect Secure / Pulse Policy Secure 9.0RX
  https://kb.PulseSecure.net/articles/Pulse_Security_Advisories/SA44101
- 複数の SSL VPN 製品の脆弱性に関する注意喚起
  https://www.jpcert.or.jp/at/2019/at190033.html
- Over 14,500 Pulse Secure VPN endpoints vulnerable to CVE-2019-11510
  https://BadPackets.net/over-14500-pulse-secure-vpn-endpoints-vulnerable-to-cve-2019-11510/
- Infiltrating Corporate Intranet Like NSA - Pre-auth RCE on Leading SSL VPNs
  https://www.blackhat.com/us-19/briefings/schedule/#infiltrating-corporate-intranet-like-nsa---pre-auth-rce-on-leading-ssl-vpns-15545
- 2019/11/05 14:08 の @bad_packets によるツイート
  https://twitter.com/bad_packets/status/1191839806432526337
- ローカルキャッシュマネジメントサービスの通信暗号化装置への不正アクセスによる台湾拠点の一部お客さま情報および第三者情報の漏えいについて
  https://www.bk.mufg.jp/news/news2019/pdf/news1025.pdf
- CVE-2019-11510 : Pulse Connect Secureで任意のファイルアクセスを実行するための概念実証
  https://jp.tenable.com/blog/cve-2019-11510-proof-of-concept-available-for-arbitrary-file-disclosure-in-pulse-connect-secure
- Potential pre-auth RCE on Twitter VPN
  https://hackerone.com/reports/591295
- 三菱UFJ銀行が不正アクセスを受けた通信暗号化装置について調べてみた
  https://piyolog.hatenadiary.jp/entry/2019/10/29/060335
- 脆弱性対策の効果的な進め方 ツール活用編
  https://www.ipa.go.jp/topic/isec-technicalwatch-201902.html

© 2021 NTT DATA INTELLILINK Corporation

NTT DATA

Trusted Global Innovator

© 2021 NTT DATA INTELLILINK Corporation