2022 年 03 月 23 日

サービス＆セキュリティ株式会社 e-Gate センター

注意喚起：VPN 装置の脆弱性を悪用した攻撃とその対策について

1. 概要

2022 年 2 月末に、情報処理推進機構（IPA）から 2021 年下半期の「コンピュータウイルス・不正アクセスの届出事例」が公開されました。その中で、不正アクセスの足掛かりとして VPN 装置の脆弱性を悪用した事例が多数報告されています。

コロナ禍によるテレワーク環境の継続の中、VPN によって社外から内部ネットワークに接続するケースも多く、VPN 機器に対する攻撃への対策は必須と言えます。

今回はそのような VPN 装置の脆弱性を悪用した攻撃の手法とその対策についてご紹介いたします。

2. VPN 装置の脆弱性の事例（CVE-2018-13379）

攻撃に悪用される VPN 装置の脆弱性の一例として、Fortinet 社製 FortiOS の SSL VPN 機能の脆弱性（CVE-2018-13379）が挙げられます。脆弱性自体は 2019 年に公開されたものであり、すでに脆弱性を修正したバージョンが公開されていますが、この脆弱性をついた攻撃を e-Gate センターでは現在でも継続して検知しています。

この脆弱性は第三者が任意のファイルを読み取れるようになるものであり、VPN 接続を行うユーザ名やパスワードの情報を含むファイルを窃取することができます。対象システムは下記のバージョンです。

・FortiOS 6.0.0 から 6.0.4 までのバージョン
・FortiOS 5.6.3 から 5.6.7 までのバージョン
・FortiOS 5.4.6 から 5.4.12 までのバージョン

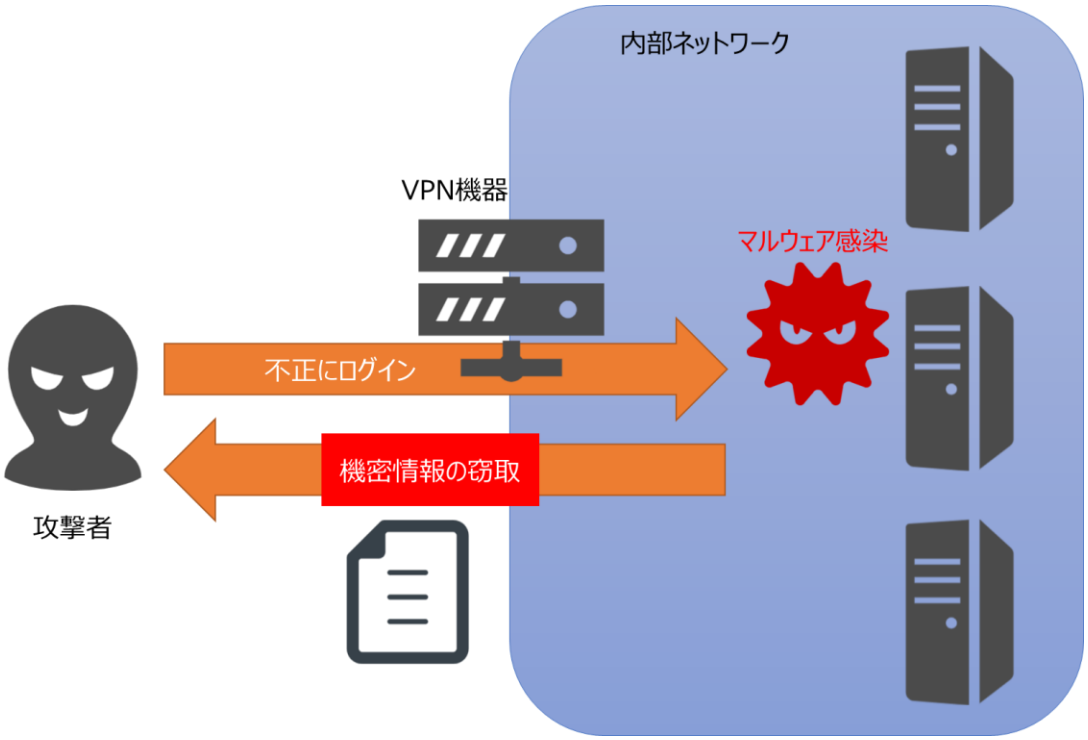
【図 1】VPN 装置の脆弱性をついた攻撃による認証情報窃取のイメージ

3. 攻撃による被害

VPN 装置への攻撃により、本来権限を持たない第三者が認証情報を手に入れて不正な VPN 接続を行うことができるようになります。VPN 接続で内部ネットワークに侵入した攻撃者は、サーバや端末をマルウェアに感染させたり、機密情報を窃取したりすることができるようになります。

実際に IPA が公開している攻撃の事例においても、まず VPN 機器への攻撃により認証情報を窃取し、内部ネットワークに侵入を行い、内部サーバをランサムウェアに感染させ、結果としてシステムが停止するなどの被害を及ぼした事例が多数見られます。また、窃取された認証情報はダークウェブで公開されるなど、攻撃者の格好の標的にされています。一度認証情報が窃取されてしまうと、様々な攻撃者からの攻撃の対象になるリスクを抱えてしまうといえます。

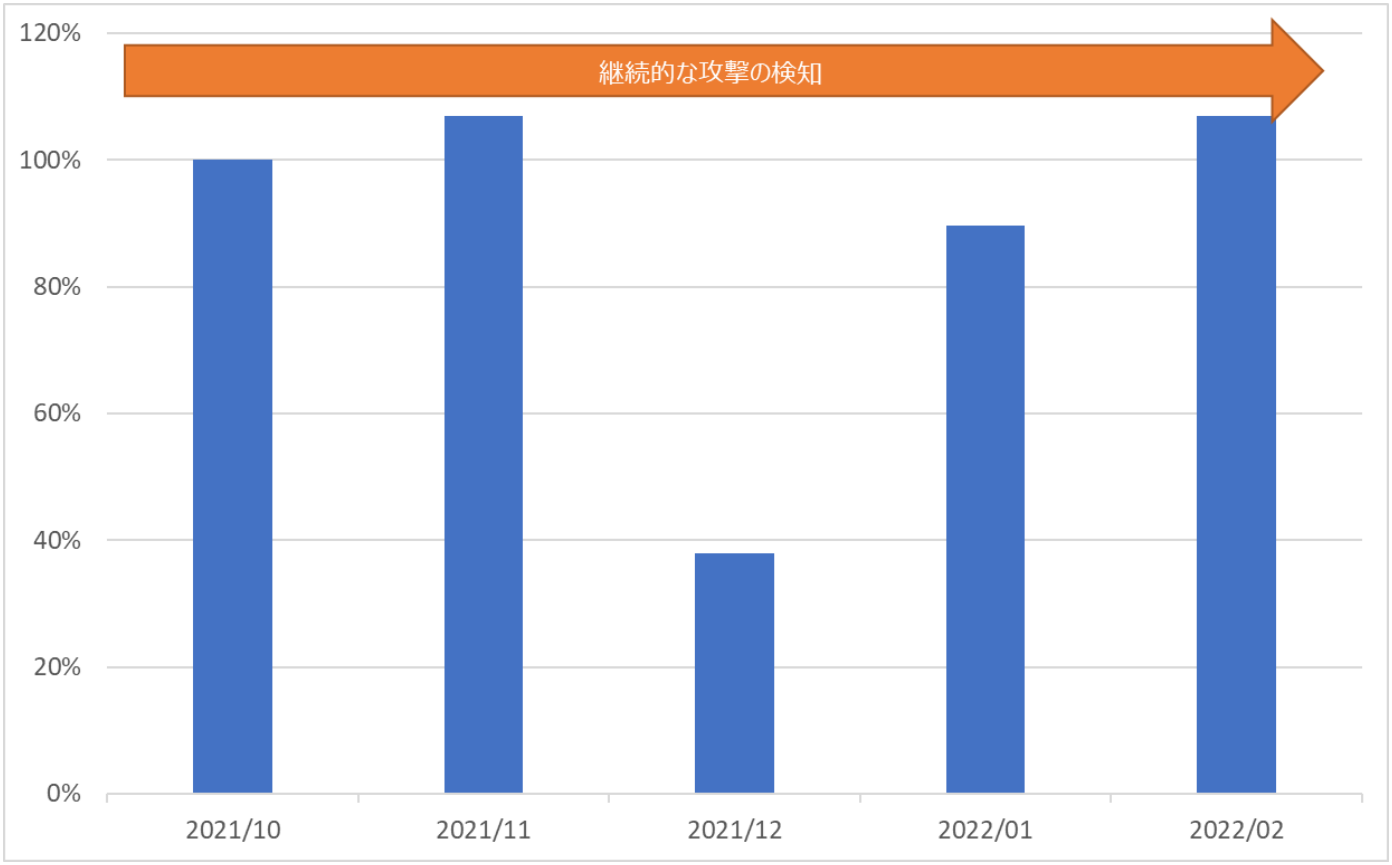
実際に攻撃を受けてしまった場合、すべてのユーザアカウント情報を窃取されている可能性があるため、脆弱性を解消した後に全ユーザアカウントのパスワードをリセットする対応が必要になります。



【図 2】不正な VPN 接続による攻撃のイメージ

4. e-Gate センターにおける攻撃検知

e-Gate センターでは VPN 装置の脆弱性をついた攻撃を継続的に検知しています。下図は 2021 年 10 月以降の CVE-2018-13379 への攻撃を含む VPN 関連イベントの検知数の推移です。全体を通して顕著な増加傾向こそ見られないものの、VPN 装置の脆弱性への攻撃が継続的に行われていることを示しています。



【図 3】e-Gate センターにおける VPN 関連イベント数の推移（2021 年 10 月度を 100%として算出）

5. 攻撃対策

攻撃対策については以下の方法があります。

・最新アップデートの適用

開発元より公開されている脆弱性を修正したバージョンへのアップデートが推奨されます。

・VPN 機能の無効化

VPN 機能を使用していない場合は無効化することにより、不正なログインは行われなくなります。

・二要素認証の実装

二要素認証の実装により不正なログインのリスクを抑えることができます。

・パスワードの変更

脆弱性のある状態で VPN 機器を使用していた場合、アップデートの適用によって脆弱性が解消された後でも、適用前にすでに認証情報が窃取されている可能性を考慮し、パスワード等の認証情報を変更する必要があります。

・セキュリティ機器による攻撃通信の監視

Firewall や IPS（侵入防御システム）等のセキュリティ機器により、不審な通信を検知・遮断することも一定の効果が見込めます。

6. 参考

・IPA

コンピュータウイルス・不正アクセスに関する届出について

https://www.ipa.go.jp/security/outline/todokede-j.html

・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

Fortinet 社製 FortiOS の SSL VPN 機能の脆弱性（CVE-2018-13379）の影響を受けるホストに関する情報の公開について

https://www.jpcert.or.jp/newsflash/2020112701.html

7. e-Gate の監視サービスについて

e-Gate のセキュリティ機器運用監視サービスでは、24 時間 365 日、リアルタイムでセキュリティログの有人監視を行っております。サイバー攻撃への対策としてセキュリティ機器を導入する場合、それらの機器の運用監視を行い、通信が攻撃かどうかの分析、判断をして、セキュリティインシデント発生時に適切に対処できるようにすることが重要です。e-Gate のセキュリティ監視サービスをご活用いただきますと、迅速なセキュリティインシデント対応が可能となります。

また、e-Gate の脆弱性診断サービスでは、お客様のシステムにて潜在する脆弱性を診断し、検出されたリスクへの対策をご提案させていただいております。

監視サービスや脆弱性診断サービスをご活用いただきますと、セキュリティインシデントの発生を予防、また発生時にも迅速な対処が可能なため、対策コストや被害を抑えることができます。

■総合セキュリティサービス e-Gate

SSK（サービス＆セキュリティ株式会社）が 40 年以上に渡って築き上げてきた「IT 運用のノウハウ」と最新のメソッドで構築した「次世代 SOC“e-Gate センター”」。この 2 つを融合させることによりお客様の情報セキュリティ全体をトータルにサポートするのが SSK の“e-Gate”サービスです。e-Gate センターを核として人材・運用監視・対策支援という 3 つのサービスを軸に全方位のセキュリティサービスを展開しています。

【参考 URL】

https://www.ssk-kan.co.jp/e-gate/

※本資料には弊社が管理しない第三者サイトへのリンクが含まれています。各サイトの掲げる使用条件に従ってご利用ください。
　リンク先のコンテンツは予告なく、変更、削除される場合があります。
※掲載した会社名、システム名、製品名は一般に各社の登録商標 または商標です。

«お問合せ先»
サービス＆セキュリティ株式会社
〒150-0011
東京都渋谷区東 3 丁目 14 番 15 号 MO ビル 2F
TEL 03-3499-2077
FAX 03-5464-9977
sales@ssk-kan.co.jp