2021 年 08 月 27 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：Windows 印刷スプーラーの脆弱性をついた攻撃について

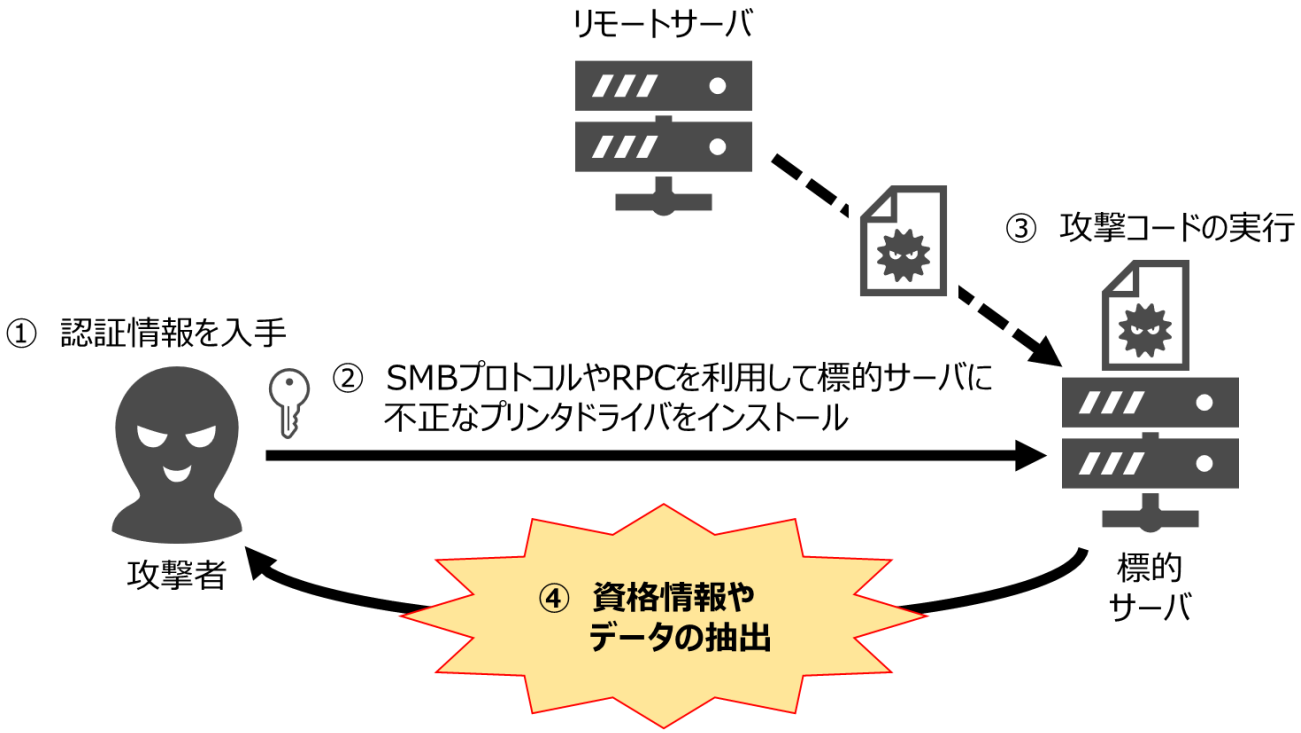
1. 概要

2021 年 6 月から 8 月にかけて Microsoft 社から Windows 印刷スプーラーにおける緊急性の高い脆弱性情報が立て続けに公開されました。その危険性から米政府が 7 月 13 日に緊急指令を発する事態となり、話題となりました。脆弱性情報の公開から 1 か月以上経過した現在でも、この脆弱性を悪用するサイバー攻撃は依然として続いており、世界中で被害が拡大しております。

今回はこの脆弱性の詳細、攻撃手法と最新の動向について紹介いたします。

2. 脆弱性の詳細 「PrintNightmare」

Windows 印刷スプーラーとは、Windows での印刷において印刷待ちを実現するためのサービスです。7 月 1 日に Windows 印刷スプーラーにリモートコード実行が可能な脆弱性（通称 PrintNightmare）が公開されましたが、すでに攻撃への悪用が確認されています。攻撃対象のサーバに対する認証情報、またはローカルネットワークへのアクセス手段を確保している場合、攻撃者は当該脆弱性を悪用し、サーバに不正アクセスして様々な攻撃をすることができます。当該脆弱性を修正する更新プログラムが公開されています。この脆弱性「PrintNightmare」を悪用した攻撃方法の一例については、図 1 のとおりとなります。



【図 1】 Windows 印刷スプーラーの脆弱性をついた攻撃方法の一例

① 攻撃者はリモートアクセスを行うための認証情報を入手します。
② 攻撃者は入手した認証情報を用いて、遠隔から SMB プロトコルもしくは遠隔手続き呼び出し(RPC：Remote Procedure call)を経由して、リモートサーバ上にある不正なプリンタドライバを標的サーバにインストールします。主に使用されるポートは 135/tcp、139/tcp、445/tcp です。
③ 標的サーバにインストールした不正なドライバにより、任意の攻撃コードが SYSTEM 権限で実行されます。
④ 攻撃者は資格情報やデータを抜き取り、漏出させます。

このように、Windows 印刷スプーラーの脆弱性を悪用されることにより、情報漏出などの被害が発生する可能性があります。その他にもランサムウェア攻撃に使用する事例も報告されています。

本脆弱性対策の更新プログラムを適用した後も、プリンタドライバなどの印刷機能に必要なファイルや構成情報を外部サーバからダウンロードしてクライアントにインストールできる「ポイントアンドプリント」機能により、非管理者権限でも攻撃が実行可能であることが確認されました。これについては 8 月 10 日の Windows アップデート適用時に、プリンタドライバのインストールとアップデートの際に管理者権限を必要とするよう動作変更したことにより対処されています。

3. 脆弱性情報公開以降の動向

2021 年 6 月 8 日（米国時間）、Windows 印刷スプーラーにローカルネットワークにおける権限昇格の脆弱性が報告されました。当初はローカルネットワークへの侵入が必要なことから悪用の可能性は低いと判定されていました。しかし、7 月 1 日にリモートコード実行が可能な脆弱性が報告され、攻撃への悪用が確認されております。さらに、Windows 印刷スプーラーの脆弱性を対象としたランサムウェア攻撃の増加が報告されるなど、世界中で被害が拡大しております。

これを受けて、Microsoft 社が Windows 印刷スプーラーの脆弱性に関する脆弱性情報の公開を立て続けに行っています。最新の情報では 8 月 11 日に新たなゼロデイ脆弱性（CVE-2021-36958）が報告され、8 月 27 日現在でも対象の OS バージョンについて調査中となっております。

6 月から 8 月（8 月 27 日現在）にかけて公開された脆弱性情報は表 1 のとおりです。このうち、色付けされているものは、攻撃への悪用事例を確認している、もしくは悪用の可能性が高いと判断されている脆弱性です。

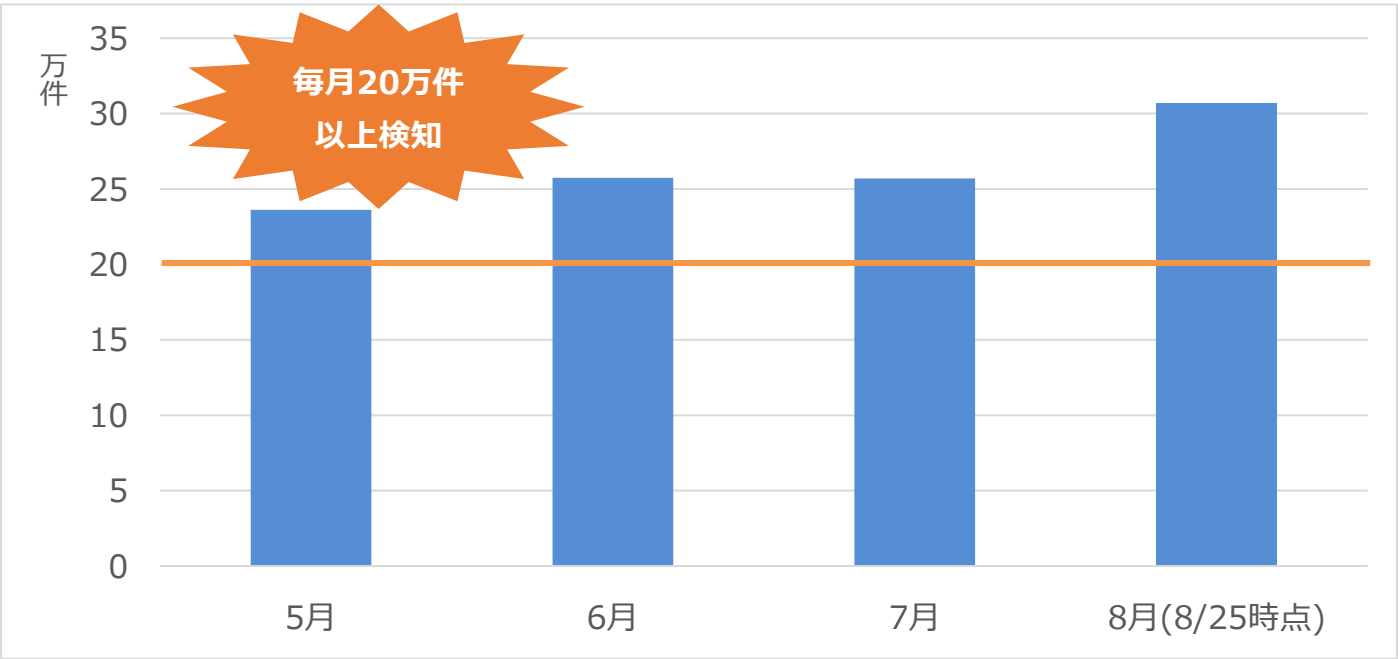
【表 1】6 月から 8 月にかけて報告された脆弱性情報

公開日	CVE ID	タイトル	CVSSv3	CVSSv2
2021 年 6 月 8 日	CVE-2021-1675	Windows 印刷スプーラーの権限が昇格される脆弱性	8.8	9.3
2021 年 7 月 1 日	CVE-2021-34527	Windows 印刷スプーラーのリモートでコードが実行される脆弱性	8.8	9.0
2021 年 7 月 15 日	CVE-2021-34481	Windows 印刷スプーラーの権限が昇格される脆弱性	7.8	4.6
2021 年 8 月 10 日	CVE-2021-36936	Windows 印刷スプーラーのリモートでコードが実行される脆弱性	9.8	7.5
2021 年 8 月 10 日	CVE-2021-36947	Windows 印刷スプーラーのリモートでコードが実行される脆弱性	8.8	6.5

公開日	CVE ID	タイトル	CVSSv3	CVSSv2
2021 年 8 月 10 日	CVE-2021-34483	Windows 印刷スプーラーの権限が昇格される脆弱性	7.8	4.6
2021 年 8 月 11 日	CVE-2021-36958	Windows 印刷スプーラーのリモートでコードが実行される脆弱性	7.8	9.3

4. e-Gate センターにおける攻撃検知の推移

e-Gate センターでは今回の脆弱性をついた攻撃の起点として狙われるポート 135/tcp、139/tcp、445/tcp への通信を継続的に多数観測しております。2021 年 5 月以降毎月 20 万件以上検知しております。8 月については 8 月 25 日時点で 30 万件以上検知しており、前月に比べて増加傾向にあるため、より注意すべき状況となっております。実際の推移観測結果が図 2 のとおりです。



【図 2】e-Gate センターにおけるポート 135、139、445 への通信検知数の推移

5. 攻撃対策

- 最新のアップデートの適用

2021 年 8 月 10 日までの脆弱性を修正する更新プログラムを Microsoft 社が公開しています。対象バージョンのシステムを使用している場合、インストールすることが推奨されます。加えて、Microsoft 社は更新プログラムのインストール後に「ポイントアンドプリント」を無効化して、かつ非管理者アカウントがプリンタドライバをインストールできないように設定することを推奨しています。

なお、2021 年 8 月 27 日時点では CVE-2021-36958 を修正したバージョンはリリースされておらず、準備中とのことです。当該脆弱性についても修正したバージョンがリリースされ次第、インストールすることが推奨されます。

- ワークアラウンド（緩和策）の実行
  脆弱性に対するアップデートを適用できない場合の緩和策として、印刷サーバ以外の機器で Windows 印刷スプーラーを停止し無効化する方法があります。これにより当該脆弱性の影響を軽減できます。また、グループポリシーを使用して、インバウンドからのリモート印刷を無効化することでリモートからの攻撃を阻止できます。CVE-2021-36958 に対しても同様に、Windows 印刷スプーラーの無効化が緩和策となります。
- セキュリティ機器による攻撃通信の監視
  外部からのポート 135、139 及び 445 への不正アクセスを Firewall や IPS（侵入防御システム）で拒否することで、攻撃の初期段階を阻止することができます。

Windows 印刷スプーラーの脆弱性を悪用した攻撃は今後長く継続すると推測され、攻撃の被害にあう可能性があります。Firewall や IPS といったセキュリティ機器により攻撃通信を検知、防御することで、被害を最小限に抑えることができます。何よりも、いち早く攻撃に気付けるような仕組みと監視体制を徹底しておくことが有効な対策となります。

6. 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 の総合セキュリティサービス“e-Gate”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/

7. 参考情報

IPA

- 更新：Microsoft Windows 製品の Windows Print Spooler の脆弱性対策について（CVE-2021-34527）
  https://www.ipa.go.jp/security/ciadr/vul/20210705-ms.html

JPCERT/CC

- Windows の印刷スプーラーの脆弱性（CVE-2021-34527）に関する注意喚起
  https://www.jpcert.or.jp/at/2021/at210029.html

JVN

- JVNVU#96414899 Microsoft Windows の印刷スプーラーにリモートコード実行の脆弱性
  https://jvn.jp/vu/JVNVU96414899/index.html

«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