2022 年 07 月 28 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 サポート診断ツールの脆弱性「Follina」について

1. 概要

2022 年 5 月末に Windows サポート診断ツール（Microsoft Support Diagnostic Tool：MSDT）に関する脆弱性（CVE-2022-30190）が公開されました。

この脆弱性は通称 Follina と命名されており、悪用されると Word ファイルや RTF ファイルを開くまたはプレビューするだけで任意のコードが実行されてしまう恐れがあります。既に複数の攻撃者による Follina の悪用が確認されており、ユーザはいち早い修正プログラムの適用が推奨されます。今回は Follina の詳細と最新の動向について紹介いたします。

2. Follina と悪用した攻撃について

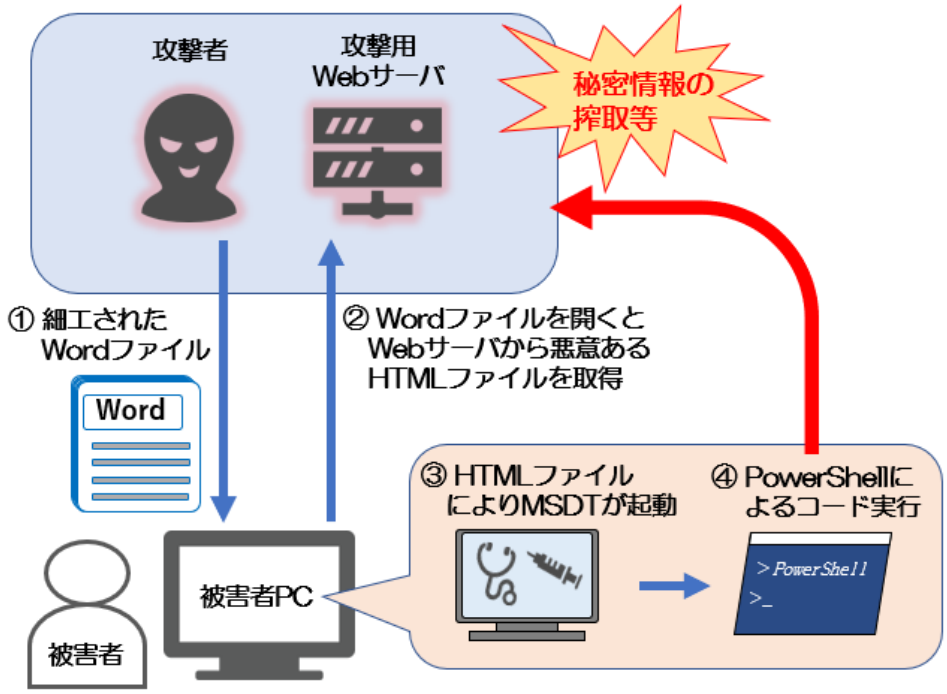
Windows サポート診断ツール（以降は MSDT と記載）は Windows 環境で問題が発生した場合、解析に必要な情報を取得し Microsoft サポートチームに送る目的で作成されたツールであり、Windows 標準アプリケーションとしてインストールされています。Follina はこの MSDT の脆弱性であり、攻撃者が細工した Word ファイルや RTF ファイルをきっかけに MSDT が呼び出され、PowerShell でコードが実行される可能性があります。

本脆弱性を悪用することで、MSDT を介した PowerShell コード実行やマルウェア感染が可能となり、最終的に秘密情報の漏洩などの被害が発生する恐れがあります。今後ものこの脆弱性を利用したさまざまな攻撃手法が確立されると、さらに被害が増える可能性もあります。

今回の脆弱性を悪用した攻撃で最も注目すべき点は、悪用の過程で Microsoft Office におけるマルウェア防御策として一般化している「マクロの無効化」では攻撃を阻止できないということです。また、エクスプローラーのプレビュー機能を有効にしていると、RTF ファイルに対してはファイルを開く事なくプレビューするだけで攻撃が成立してしまう可能性があります。しかも、Follina を悪用した攻撃が成立すると MSDT が起動しますが、MSDT は Windows の標準アプリケーションのため、これらのマルウェアの感染にまで気が付かずに、攻撃者に機密情報を長期間盗まれ続けるケースも考えられます。

Follina を悪用した攻撃の流れは下記の通りとなります。（Word ファイルを利用した攻撃手法の一例）

① 攻撃者により細工された Word ファイルが添付されたメールを被害者が受信します。
② 被害者がファイルを開くことで、Word のリモートテンプレート機能により、攻撃用の Web サーバへのアクセスが発生し、細工された悪意のある HTML ファイルを取得します。
③ 取得された悪意ある HTML ファイルにより MSDT が起動されます。
④ MSDT を経由し、PowerShell で任意のコードが実行されます。
PowerShell での悪意あるコード実行により、秘密情報の漏洩などの被害が発生する可能性があります。



【図 1】Follina を悪用した攻撃イメージ（Word ファイルの例）

3. 経緯と最新の動向

Follina は 5 月 30 日に Microsoft 社によって、その存在と悪用の事実が公表され、6 月の月例パッチによって本脆弱性の修正プログラムが配布されました。この期間、Microsoft Office における重大なゼロデイ攻撃として注目され、実際に欧州やアメリカの政府機関、チベットなどへ複数の攻撃集団が Follina を悪用したという報道がありました。

また、以下のようなマルウェアを感染させる為に Follina の悪用が確認されています。

・AsyncRAT

AsyncRAT に感染すると認証情報などを外部に送信され、端末をリモートコントロールされる恐れがあります。

・XFiles info-stealer

XFiles info-stealer は機密情報をテキストやスクリーンショットの形で窃取するマルウェアで、Telegram により窃取した情報を送信する特徴があります。

・Qbot

Qbot も XFiles info-stealer 同様に機密情報を窃取するマルウェアです。ワームとして他のコンピュータに自身を複製し増殖する機能を持ち合わせています。

・Rozena

Rozena は攻撃者からのシェルコマンドを受けつけるバックドアを作成するマルウェアです。Follina を悪用し Rozena を感染させたのち、その侵入の痕跡を隠滅するといった、高度な攻撃が確認されています。

2022 年 7 月現在 e-Gate センターでは本脆弱性を悪用した攻撃を検知しておりませんが、Follina は様々なマルウェア攻撃の玄関口の一つとされる危険性があり、警戒を強めています。

4. 対策について

本脆弱性に関しては Microsoft 社により修正プログラムが発表されています。Windows Update を有効にしていれば自動的にアップデートされます。また、何らかの事情で Windows Update を適用できない場合、Microsoft 社は回避策として MSDT URL プロトコルの無効化を案内していますのでご確認ください。（６． 参考情報を参照ください）

今後、Follina に類似(※1)した、マクロの実行を伴わず、プレビューのみで成立するといった攻撃が増加する可能性があります。このような攻撃手法に対しては、従来通りの「マクロを有効にしない」、「不審なファイルは開かない(実行しない)」という対策だけでは不十分となるため、これらを想定したセキュリティ対策を考えていくことが重要です。

まず、ユーザ単位での対策としては、以下の事柄が考えられます。

・エクスプローラーのプレビュー機能をオフする(プレビューウィンドウを表示しない)。

・ダウンロードと同時にリアルタイムスキャンをおこなう AntiVirus ツールを導入する。

・サンドボックス機能のあるメールセキュリティ製品を活用する。

また、ネットワーク上に Firewall や IPS(侵入防御システム)、UTM(統合脅威管理)といったセキュリティ機器を導入し、攻撃通信を検知、防御することも有効な対策となります。セキュリティ機器の導入後は適切な運用が必要となるため、SOC(※2)や CSIRT(※3)の自社設置やセキュリティベンダへの外部委託といった手段も有用です。

※1:マクロの実行を伴わない Office に関する脆弱性として知られる CVE-2021-40444 と Follina は仕組みが類似していることが指摘されています。CVE-2021-40444 も修正パッチが公開されていますが、今後同様の脆弱性が発見され、悪用される可能性が考えられます。

※2:SOC(Security Operation Center)とは、セキュリティ製品を監視し、サイバー攻撃の検出・分析、対策の提言を行う組織です。

※3:CSIRT(Computer Security Incident Response Team)とは、コンピュータやネットワークを監視し、問題が発生したときは原因解析・調査を行う組織です。

5. 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/

6. 参考情報

・NEC

Microsoft Word などを介して任意コード実行が可能な MSDT の脆弱性（CVE-2022-30190、Follina）の検証

https://jpn.nec.com/cybersecurity/blog/220620/index.html

・Microsoft

Microsoft Windows Support Diagnostic Tool (MSDT) Remote Code Execution Vulnerability

https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2022-30190

CVE-2022-30190 マイクロソフト サポート診断ツールの脆弱性に関するガイダンス

https://msrc-blog.microsoft.com/2022/05/30/guidance-for-cve-2022-30190-microsoft-support-diagnostic-tool-vulnerability-jp/

・BROADCOM (Symantec)

Attackers Exploit MSDT Follina Bug to Drop RAT, Infostealer

https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/follina-msdt-exploit-malware

・Cyberint

XFiles Stealer Campaign Abusing Follina

https://cyberint.com/blog/research/xfiles-stealer-campaign-abusing-follina/

・Netskope

CVE-2022-30190: New Zero-Day Vulnerability (Follina) in Microsoft Support Diagnostic Tool

https://www.netskope.com/jp/blog/cve-2022-30190-new-zero-day-vulnerability-follina-in-microsoft-support-diagnostic-tool

・Fortinet

From Follina to Rozena - Leveraging Discord to Distribute a Backdoor

https://www.fortinet.com/blog/threat-research/follina-rozena-leveraging-discord-to-distribute-a-backdoor

※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