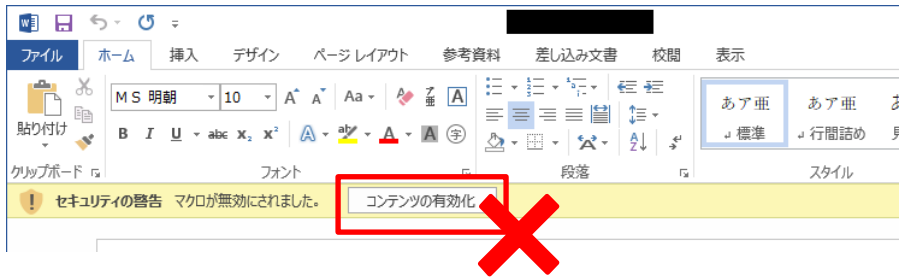
MirrorFace による攻撃への主な緩和策

TLP:GREEN

これまでに見かけなかった形式のファイルが届いた場合は、安易に添付ファイルを開かずに送信者に確認するほか、開いた後にボタンをクリックさせるなどの誘導があった際は、即座にファイルを閉じる。



- 送信元名やメールアドレスが過去のやりとりと同じでも、上記のような「いつもと違うような…」という違和感があれば、送信元に確認する。

利用しているネットワーク機器の脆弱性に関する情報収集を怠らず、適切に修正プログラムを適用する。


サイバー警察局便り
Cyber Police Agency Letter R6(2024) Vol.12

Fortinet社製品を利用している皆様へ

FortiManagerの脆弱性情報が公開されました(CVE-2024-47575)

公開された脆弱性が放置されたままだと、攻撃者に悪用され、外部から任意のコード又はコマンドを実行される可能性があります。

【影響を受けるシステム／バージョン】
- FortiManager：7.6.0、7.4.0～7.4.4、7.2.0 ～ 7.2.7、7.0.0 ～ 7.0.12、6.4.0 ～ 6.4.14、6.2.0～6.2.12
- FortiManager Cloud：7.4.1 ～ 7.4.4、7.2.1 ～ 7.2.7、7.0.1 ～ 7.0.12、6.4系の全バージョン
- FortiAnalyzer：1000E、1000F、2000E、3000E、3000F、3000G、3500E、3500F、3500G、3700F、3700G、3900E

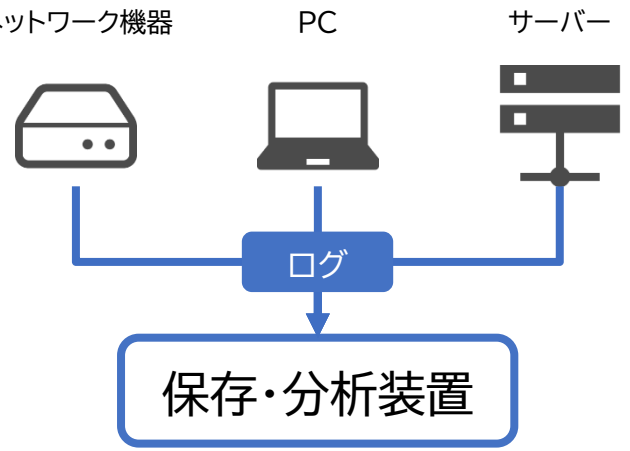
【推奨される対策】
・脆弱性が修正されたバージョンに更新する。
・修正されたバージョンへの更新が困難な場合は下記のFortinet社のページに記載された回避策の適用を検討する。
※最新の情報及び詳細はFortinet社のページ(https://fortiguard.fortinet.com/psirt/FG-IR-24-423)を参照

被害に遭った場合は、最寄りの警察署又は都道府県警察本部のサイバー犯罪相談窓口に通報・相談してください！
都道府県警察本部のサイバー犯罪相談窓口はこちら⇒ https://www.npa.go.jp/bureau/cyber/soudan.html

警察庁 National Police Agency
ランサムウェア対策、不正アクセス対策等のほか、サイバー事案に関する相談対応等を掲載しています。⇒https://www.npa.go.jp/bureau/cyber/index.html

- 上記は警察庁による注意喚起例。
- 実害が把握できていない場合も、密かに侵入・侵害されている可能性。

広範囲かつ長期間にわたってログを保存・管理する。



- ログは、侵害の原因と範囲の把握に不可欠。
- 被害認知まで2～3年かかる例もあり、原因や被害範囲が特定できず、対策が不十分となる。

正規のソフトウェアを悪用した新たな手口

「Windows サンドボックス」(隔離環境実現用ソフト)や、「Visual Studio Code」(プログラム開発用ソフト)といった、正規のソフトウェアが悪用され、被害者に気づかれないように不正プログラム(マルウェア)の実行や、遠隔操作が可能。

勝手に有効化・実行されていないか、定期的に確認することを推奨。