おまかせサイバーみまもり

2023年10月　セキュリティ対応状況と検知状況

2023年11月
東日本電信電話株式会社

セキュリティ対応状況

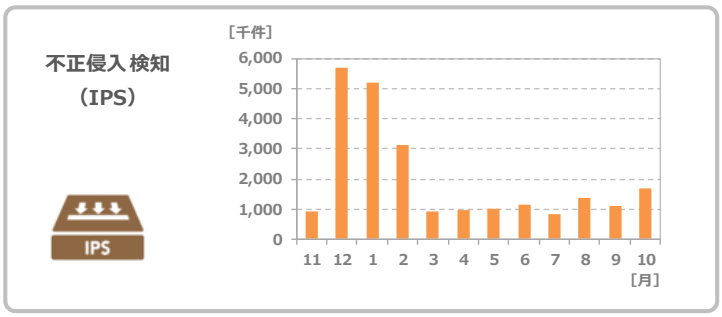
2023年10月10日（現地時間）に、Fortinet社より重要度が5段階中もっとも高い「クリティカル」を含む脆弱性が24件公表されています。UTM（FortiGate）に関する脆弱性も6件あり、SSLディープインスペクションに関連する脆弱性「CVE-2023-41675」が含まれております。本脆弱性を悪用された場合、認証されていないリモートの攻撃者が、一定の条件を満たすポリシーに一致する複数の細工されたパケットを送信することで、Webプロキシプロセスをクラッシュさせる可能性があります。 クラッシュしたWebプロキシプロセスは短時間で再起動しますが、一時的なDoS攻撃の目的で悪用される恐れがあります。影響を受けるバージョンは、FortiOS 7.0.0～7.0.10、FortiOS 7.2.0～7.2.4となります。バージョンアップ計画策定の参考の一助となれば幸いです。

■参考　Fortinet社　https://www.fortiguard.com/psirt/FG-IR-23-184

セキュリティ検知状況

- おまかせサイバーみまもり専用BOXで検知したアラート数をNTT東日本が集計
- 集計期間：2022年11月～2023年10月

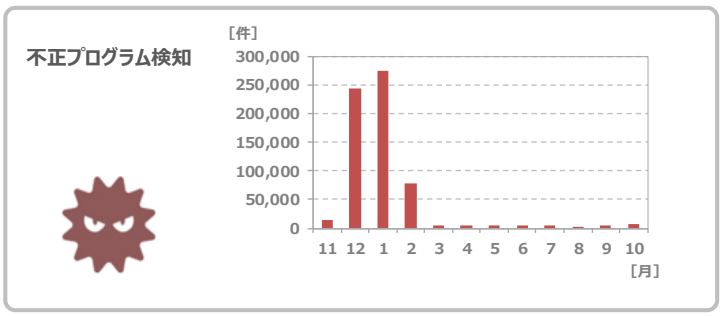
不正侵入検知



直近12カ月平均：1,989,251件
2023年10月：1,680,394件

直近12カ月の月平均に比べ低い検知状況が継続しています。
引き続きサーバ等を公開する際には十分にセキュリティ対策を実施してください。

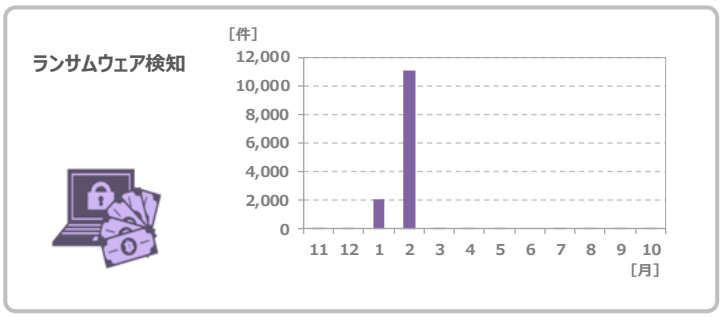
不正プログラム検知



直近12カ月平均：53,785件
2023年10月：6,161件

直近12カ月の月平均に比べ低い検知状況が継続しています。
Emotetなどの不正プログラムについては、引き続き十分に注意してください。

ランサムウェア検知



直近12カ月平均：1,106件
2023年10月：01件

直近12カ月の月平均に比べ低い検知状況が継続しています。
ランサムウェアには、引き続き十分に注意してください。