Distributed via @police https://www.npa.go.jp/cyberpolice/

令和2年3月 25 日

レポート

Apache Tomcat の脆弱性(CVE-2020-1938)を標的としたアクセスの観測等について

- Apache Tomcat の脆弱性(CVE-2020-1938)を標的としたアクセスの観測について
- 宛先ポート 9530/TCP に対する Mirai ボットの特徴を有するアクセスの増加

1 Apache Tomcat の脆弱性(CVE-2020-1938)を標的としたアクセスの観測について

令和2年2月 24 日 Apache Tomcat の脆弱性(CVE-2020-1938)に関する情報が、Apache Software Foundation より公開[i]されました。当該脆弱性が悪用された場合、遠隔から攻撃者により情報の窃取や、任意のコードを実行されるなどの可能性があります。また海外の共有ウェブサービスにおいて、当該脆弱性を対象とした PoC[ii] が公開されていることを確認しました。

警察庁のインターネット定点観測において、令和2年2月 21 日に宛先ポート 8009/TCP に対するアクセスの急増を観測しました(図1)。

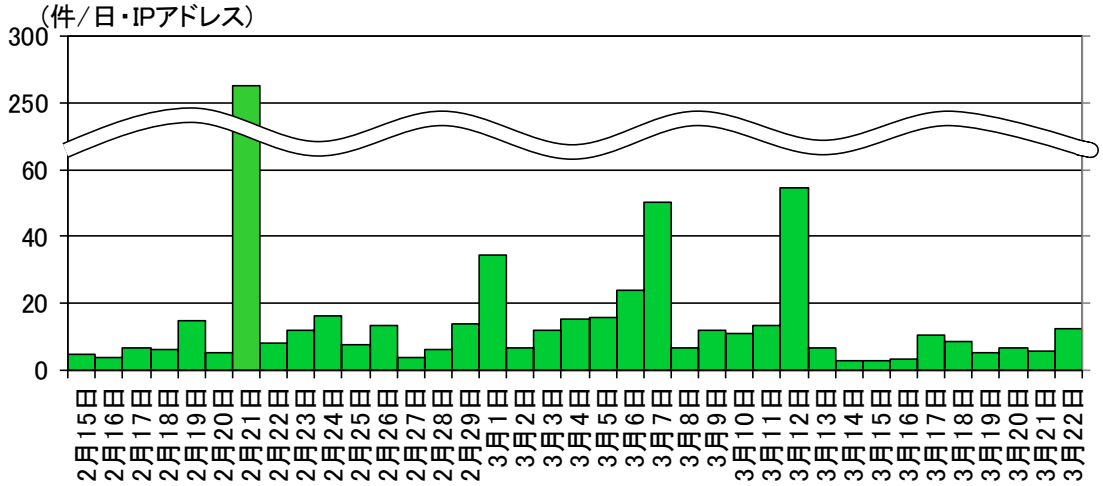

図1 宛先ポート 8009/TCP に対するアクセス件数の推移(R2.2.15～R2.3.9)

観測したアクセスの大半は脆弱性スキャンツールを利用したものと思料されるアクセスであり、令和2年2月 21 日以降、一部に PoC に関連するアクセスを観測しました。

このアクセスは、本来は外部からアクセスできないファイルに対して、脆弱性の存在する環境の場合にアクセスできることを確認するためのものでした(図2)。

---

[i] [SECURITY] CVE-2020-1938 AJP Request Injection and potential Remote Code Execution
https://lists.apache.org/thread.html/r7c6f492fbd39af34a68681dbbba0468490ff1a97a1bd79c6a53610ef%40%3Cannounce.tomcat.apache.org%3E

[ii] Proof of Concept の略。脆弱性を利用した攻撃が可能であることを示すための検証用プログラム。

図2　PoC に関連するアクセスの例（一部マスキングを実施）

Apache Tomcat の利用者は、バージョンの確認を実施してください。脆弱性のあるバージョンは、以下のとおりです。

- Apache Tomcat 9.0.0.M1 から 9.0.30
- Apache Tomcat 8.5.0 から 8.5.50
- Apache Tomcat 7.0.0 から 7.0.99

使用している Apache Tomcat のバージョンが脆弱性の影響を受けることが判明した場合には、以下の対策を実施してください。

- 開発元から公開されているセキュリティパッチの適用を実施してください。
- AJP [i] が不要な場合は、無効にしてください。
- AJP が必要な場合は、認可設定などアクセス制限をしてください。また、必要な IP アドレスのみにアクセスを許可する、VPN を用いて接続することも検討してください。

[i] Apache Jserv Protocol：クライアントから Apache を経由して Tomcat へリクエストを送信するためのプロトコル。

2　宛先ポート 9530/TCP に対する Mirai ボットの特徴を有するアクセスの増加

警察庁のインターネット定点観測において、令和2年2月 11 日頃から宛先ポート 9530/TCP に対するアクセスの増加を観測しました。当該アクセスは、宛先 IP アドレスと TCP シーケンス番号[i] の初期値が一致する Mirai ボットの特徴を有しています（図3）。

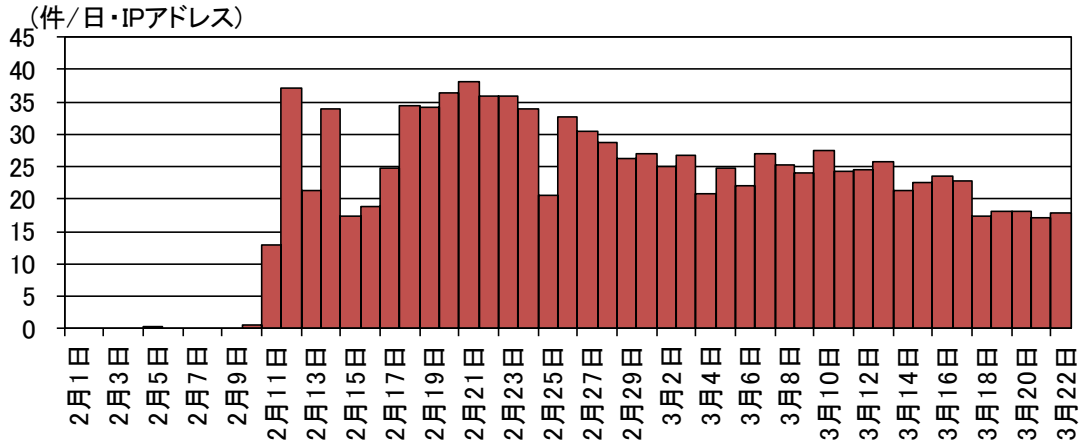

図3　宛先ポート 9530/TCP に対する Mirai ボットの特徴を有するアクセス件数の推移
（R2.2.1～R2.3.9）

観測したアクセスの中には、特定の文字列が含まれていました（図4）。海外の共有ウェブサービスにおいて、当該アクセスと関連する PoC が公開されていることを確認しました。これらのアクセスは、特定のネットワークカメラに対してリモートから文字列を送信することにより、管理者権限を窃取し Telnet で接続することができる脆弱性を調査するものとみられます。

```
.OpenTelnet:OpenOnce.
```

図4　観測したアクセスの例

このアクセスの同一送信元 IP アドレスからは、23/TCP、80/TCP、81/TCP 等を宛先ポートとするアクセスも観測していることから、不正プログラムに感染したボットが感染拡大を意図して、宛先ポート 9530/TCP を使用する IoT 機器を感染対象にしているものと考えられます。

[i] TCP パケットの送受信状況を管理するための番号で、通常は TCP 通信の開始時にランダムな番号が初期値として設定され、進行に合わせて増加します。また、この初期値を特に ISN（Initial Sequence Number）といいます。

IoT 機器の利用者は、以下の対策を参考に、総合的にセキュリティ対策を行うことを推奨します。

- 製造元のウェブサイト等で周知される脆弱性情報に注意を払い、脆弱性が存在する場合にはファームウェアのアップデートや、必要な設定変更等の適切な対策を速やかに実施してください。
- 製品によっては、ファームウェアの自動アップデート機能が存在するものもあります。このような製品を使用している場合には、同機能を有効にしてください。
- IoT 機器をインターネットに接続する場合には、直接インターネットに接続せずに、ルータ等を使用してください。
- インターネットからのアクセスを許可する場合は、必要なポートのみに限定してください。また、必要な IP アドレスのみにアクセスを許可する、VPN を用いて接続することも検討してください。
- ユーザ名及びパスワードは初期設定のままで使用せず、必ず変更してください。また、ユーザ名及びパスワードを変更する際は、推測されにくいものにしてください。
- 製造終了から年月が経過した製品は、製造元のサポートが終了し、脆弱性への対応が実施されない場合があります。そのような製品を使っている場合には、サポート中の製品への更新を推奨します。