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

令和２年 12 月 24 日

レポート

Oracle WebLogic Server の脆弱性（CVE-2020-14882）を標的としたアクセスの観測等について

- Oracle WebLogic Server の脆弱性（CVE-2020-14882）を標的としたアクセスの観測
- 宛先ポート 5501/TCP に対する Mirai ボットの特徴を有するアクセスの増加

１　Oracle WebLogic Server の脆弱性（CVE-2020-14882）を標的としたアクセスの観測

Oracle WebLogic Server は Oracle 社が開発販売するソフトウェア製品であり、Java EE でウェブアプリケーションを作成する際に利用されるアプリケーションサーバです。令和2年 10 月 21 日、Oracle WebLogic Server に存在する脆弱性（CVE-2020-14882）[i] が公表されました。当該脆弱性は、遠隔の攻撃者に不正な操作をされる可能性があります。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 10 月 29 日以降、Oracle WebLogic Server を標的としたアクセスの増加を観測しています（図1）。

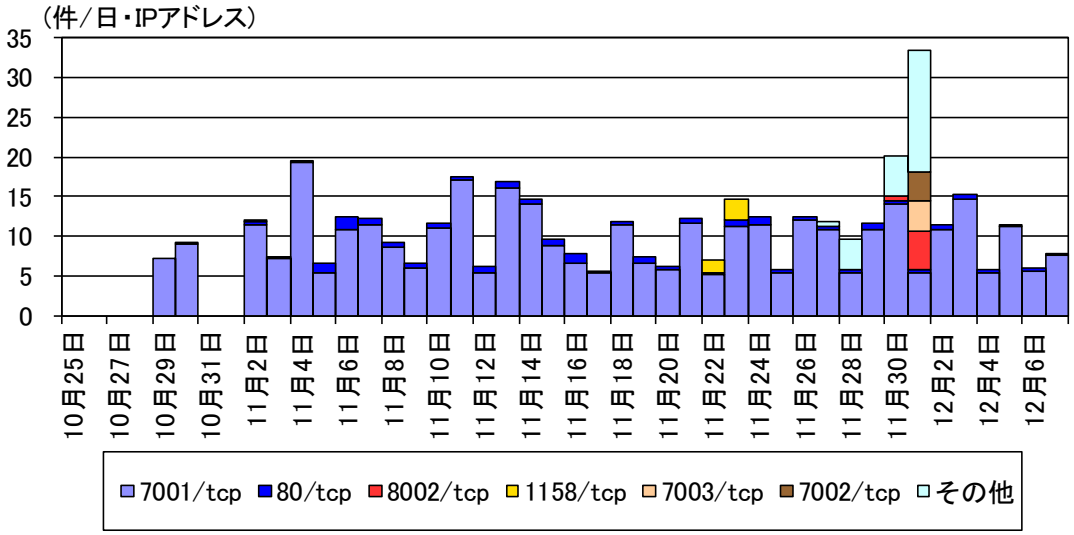

図１　Oracle WebLogic Server を標的としたアクセス件数の推移（R2.10.25～R2.12.7）

また、これらのアクセスのうち、10 月 30 日以降は、宛先ポート 80/TCP 及び 7001/TCP に対して、当該脆弱性を悪用し不正にコマンドの実行を試みるアクセスを観測しています（図2）。

[i] NVD-CVE-2020-14882
https://nvd.nist.gov/vuln/detail/CVE-2020-14882

[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。

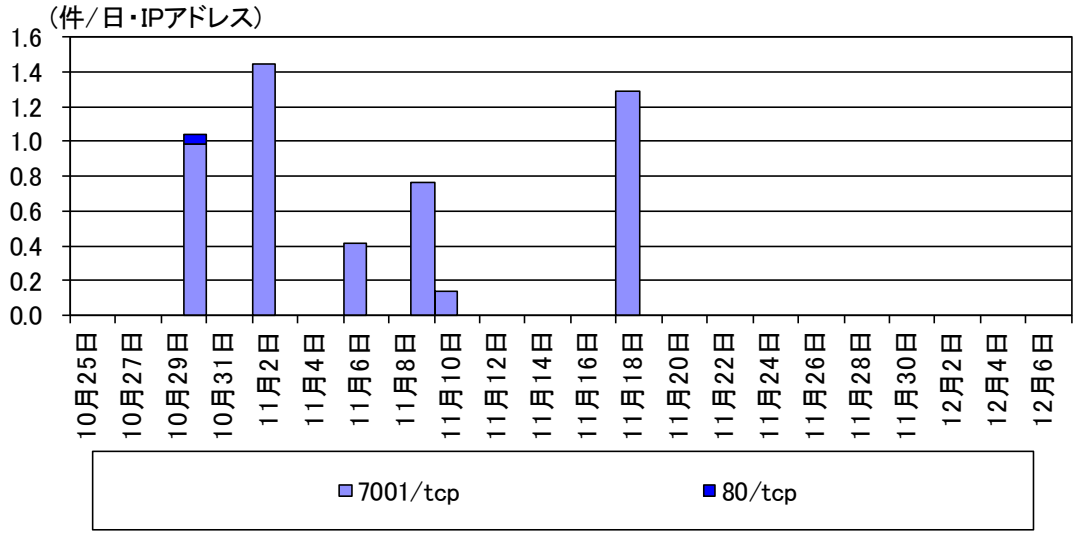

図2　Oracle WebLogic Server の脆弱性（CVE-2020-14882）を悪用したアクセス件数の推移（R2.10.25～R2.12.7）

観測したアクセスには、外部サーバから不正プログラムのダウンロード及び実行を試みるものが含まれていました（図3）。

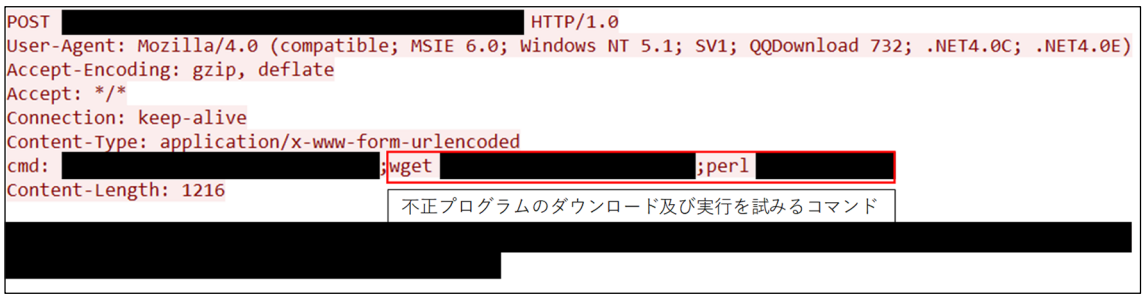

図3　Oracle WebLogic Server の脆弱性（CVE-2020-14882）を悪用したアクセスの例（一部マスキングを実施）

なお、観測により確認できた不正プログラムのファイル名とそのハッシュ値は表1のとおりです。

表1　ダウンロードされる不正プログラムのファイル名とハッシュ値

ファイル名	ハッシュ値（MD5）
bo	848bb49d6dec4fa7add65c0e6377ea77

Oracle WebLogic Server 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。

- Oracle WebLogic Server 10.3.6.0.0
- Oracle WebLogic Server 12.1.3.0.0
- Oracle WebLogic Server 12.2.1.3.0
- Oracle WebLogic Server 12.2.1.4.0
- Oracle WebLogic Server 14.1.1.0.0

使用している Oracle WebLogic Server 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。

- Oracle 社から当該脆弱性の修正プログラムを入手し、アップデートの実施を検討してください。
- Oracle WebLogic Server の管理用に利用される 7001/TCP 等、一般の利用者がアクセスする必要がないポートについては、インターネットからのアクセスを遮断する又は特定の IP アドレスからのみアクセスを許可する等の適切なアクセス制限を実施してください。
- アップデートされないまま管理用ポートがインターネットからアクセス可能となっていた Oracle WebLogic Server は、既に攻撃を受けている可能性があります。該当するサーバ等に不審なプロセス、ファイル、通信等が存在しないか確認してください。

2 宛先ポート5501/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 10 月下旬より宛先ポート 5501/TCP に対するアクセスの増加を観測しました。このアクセスは、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4)。

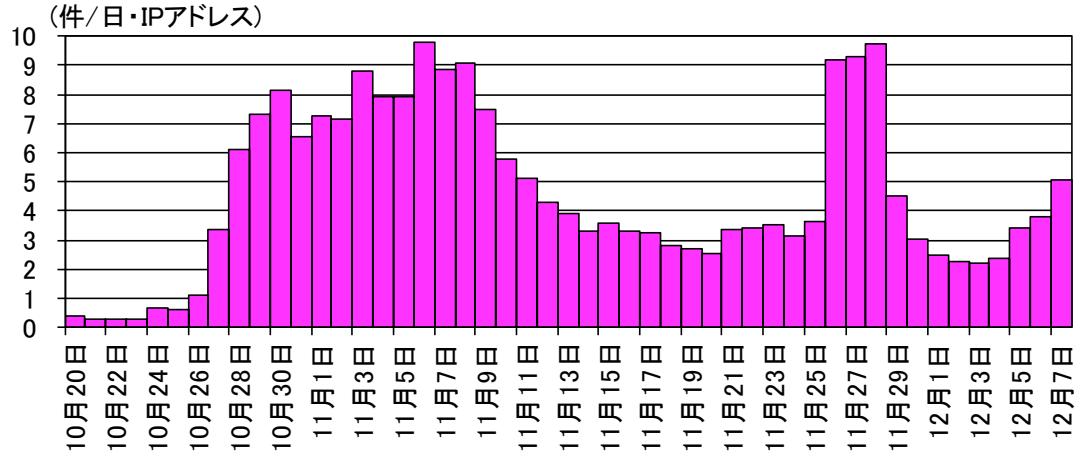

図4 宛先ポート 5501/TCP に対する Mirai ボットの特徴を有するアクセス件数の推移
(R2.10.20～12.7)

観測した宛先ポート 5501/TCP に対するアクセスの多くは、外部サーバから不正プログラムのダウンロード及び実行を試みるものでした(図5)。

図5 観測した宛先ポート 5501/TCP に対するアクセスの例(一部マスキングを実施)

[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。

同アクセスの送信元IPアドレスを調査したところ、海外製デジタルビデオレコーダ等のIoT機器のログイン画面が表示されることを確認しました（図6）。海外製デジタルビデオレコーダ等の脆弱性を悪用し、不正プログラムの感染拡大を狙ったものと考えられます。

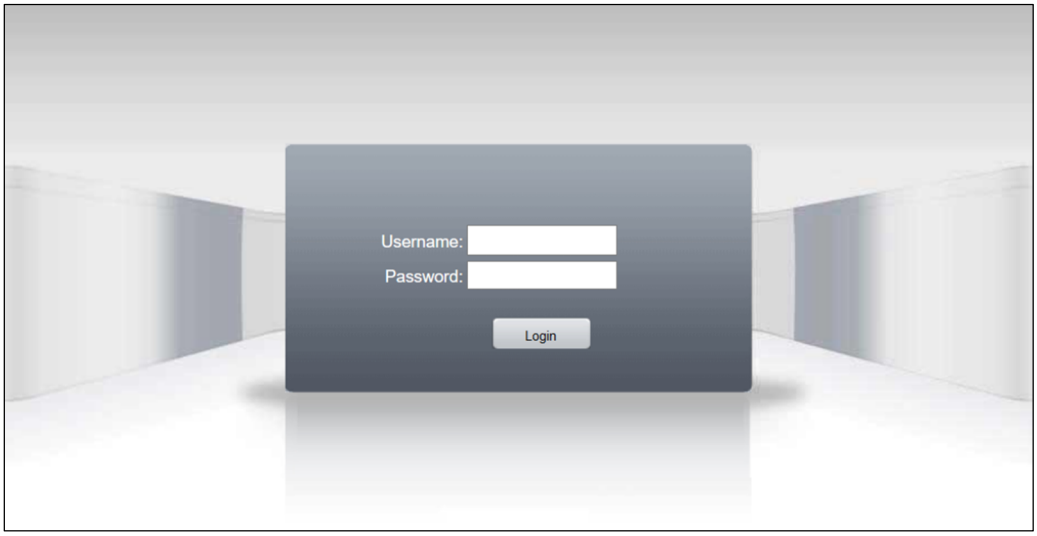

図6　海外製デジタルビデオレコーダのログイン画面の例

海外製デジタルビデオレコーダや 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したり、VPN を用いて接続することも検討してください。
- 必要がない限りは、ルータの UPnP 機能を無効にしてください。
- 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。