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

平成 27 年 12 月 25 日

インターネット観測結果等

（平成 27 年 11 月期）

- WebLogic Server を標的としたアクセスの観測
- vBulletin の脆弱性探索が目的と考えられるアクセスの観測

1 WebLogic Server を標的としたアクセスの観測

1-1 WebLogic Server の脆弱性探索を目的としたアクセス

今期は、Java アプリケーションサーバである WebLogic Server の脆弱性探索を目的と考えられる 7001/TCP に対するアクセスを観測しました。当該ポートは、WebLogic Server の初期設定で管理コンソールに使用されるポートです。

この脆弱性は Java 言語ライブラリのひとつである Apache Commons Collections の脆弱性[i]に起因するものであり、WebLogic Server も同脆弱性の影響を受けます。また、当該脆弱性が存在する WebLogic Server を探索可能なツールが公開されていることを確認しています。

11 月 13 日に警察庁の定点観測システムにおいて同脆弱性を探索するアクセスを観測したため、注意喚起[ii]を実施しました。その後も同様のアクセスを観測しました（図 1）。

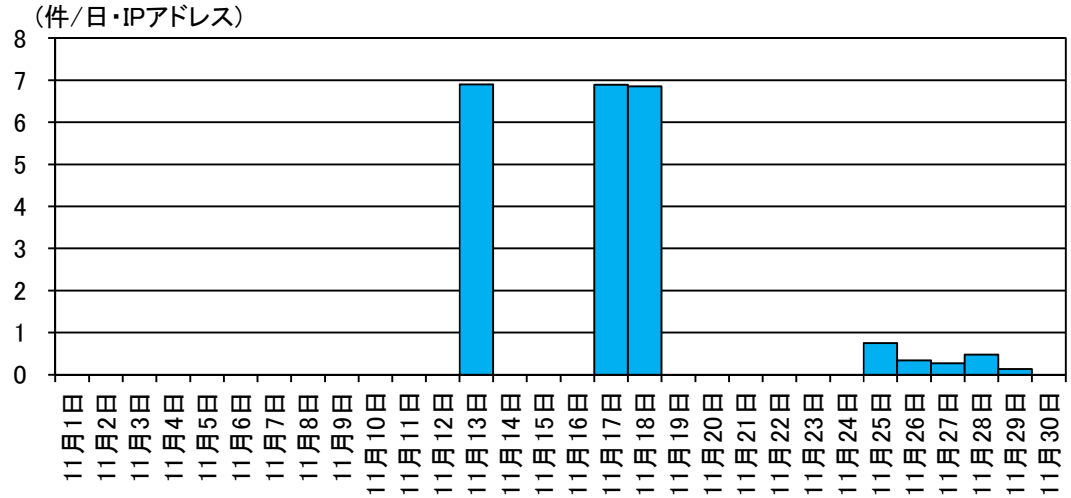

図 1 WebLogic Server の脆弱性探索が目的と考えられるアクセス件数の推移

[i] 「Apache Commons Collections ライブラリのデシリアライズ処理に脆弱性」
https://jvn.jp/vu/JVNVU94276522/

[ii] 「「WebLogic Server」の脆弱性探索が目的と考えられるアクセスの観測について」（平成 27 年 11 月 15 日）
http://www.npa.go.jp/cyberpolice/topics/?seq=17214

観測したパケットの内容を確認したところ、いずれも当該脆弱性を探索するツールで使用されている文字列を含んでおり、複数の発信元から同様の手法で探索が行われている可能性が考えられます。

当該脆弱性に対する対策等については、前述の注意喚起を参照してください。

1-2 WebLogic Serverの管理コンソールの探索を目的とするアクセス

定点観測システムにおいては、脆弱性の探索を目的としたアクセスの他、WebLogic Server の管理コンソールの探索が目的と考えられる 7001/TCP に対するアクセスを観測しました（図 2）。

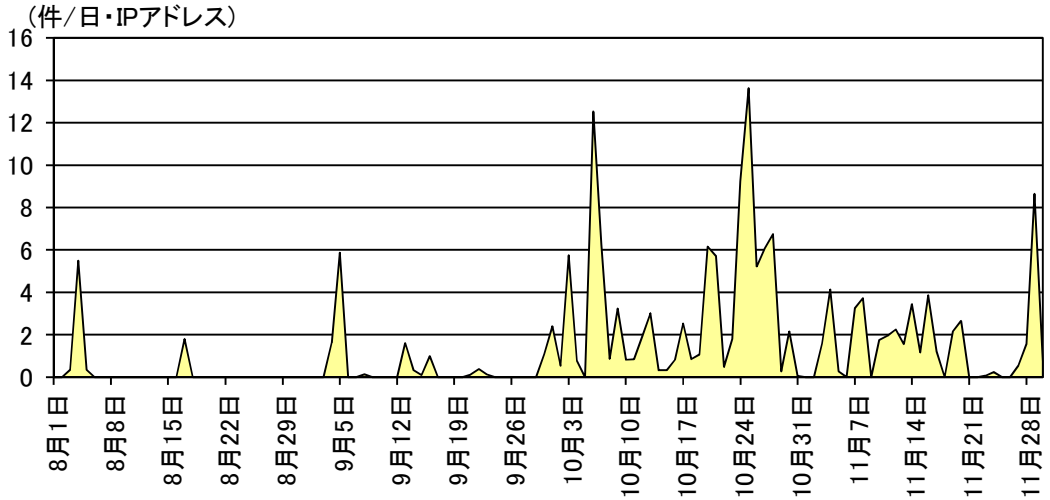

図 2 WebLogic Server の管理コンソールの探索を目的としたアクセス件数の推移
（H27.8.1～H27.11.30）

このアクセスは、アクセス可能な WebLogic Server の管理コンソールを探索するものであり、8月上旬に初めて観測し 10 月に増加した後も継続して観測しています。

WebLogic Server の管理コンソールを探索するツールがインターネット上に公開されていること確認しています。

2　vBulletin の脆弱性探索が目的と考えられるアクセスの観測

vBulletin は、PHP で稼動するフォーラム形式の掲示板ソフトウェアであり、海外で広く普及しています。

11 月３日に、リモートから任意のコードを実行される危険性がある脆弱性[i]が公表されており、開発元からは、当該脆弱性に対する修正プログラムが公開されています。また、ある攻撃者が当該脆弱性を悪用して vBulletin 公式サイトに侵入したとの情報[ii]も確認してます。

定点観測システムでは、11 月 10 日に、vBulletin の脆弱性の探索が目的と考えられる宛先ポート 80/TCP に対するアクセスを観測しました（図 3）。

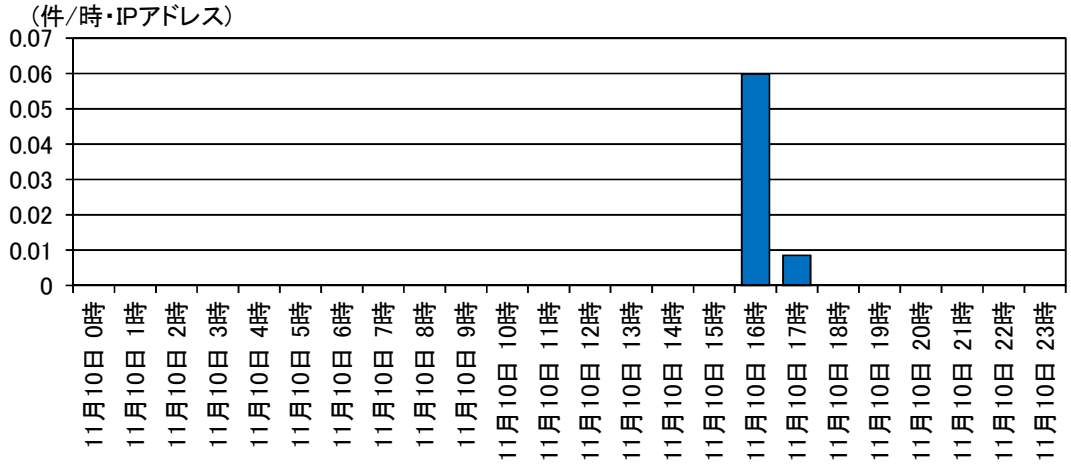

図 3　vBulletin の脆弱性探索が目的と考えられるアクセス件数の推移（11 月 10 日）

観測したパケットの内容を確認したところ、脆弱性が存在する機能に対してアクセスを試みているものでした。

---

[i] 「vBulletin 5 Connect の vB_Api_Hook::decodeArguments メソッドにおける PHP オブジェクトインジェクション攻撃を実行される脆弱性」
http://jvndb.jvn.jp/ja/contents/2015/JVNDB-2015-006017.html

[ii] 「vBulletin password hack fuels fears of serious Internet-wide 0-day attacks」
http://arstechnica.com/security/2015/11/vbulletin-password-hack-fuels-fears-of-serious-internet-wide-0-day-attacks/
「脆弱な vBulletin が稼働しているサーバーをさかんに探っているサイバー犯罪者に備え、今すぐパッチの適用を!」
http://www.symantec.com/connect/ja/blogs/vbulletin