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

平成 29 年 10 月 17 日

Topic

Apache Tomcat の脆弱性（CVE-2017-12617）を標的としたアクセスの観測について

Apache Tomcat の脆弱性（CVE-2017-12617）を標的とするアクセスを観測しました。当該脆弱性の影響を受けるウェブサーバの探索活動が実施されている可能性があるため、ウェブサーバの管理者等は影響有無の確認及び適切な対策を、早急に実施することを推奨します。

1 Apache Tomcat の脆弱性（CVE-2017-12615、CVE-2017-12617）について

Apache Tomcat は、Java で Java サーブレット及び JSP（JavaServer Pages）と呼ばれる動的なウェブページを構築する際に使用されるソフトウェア（サーブレットコンテナ）です。

平成 29 年9月 19 日に、Apache Tomcat に存在する深刻な脆弱性（CVE-2017-12615）が開発元から公表[i]されました。開発元によると、当該脆弱性が悪用された場合、攻撃者が JSP ファイルをアップロードして実行することにより、ウェブサーバ上で任意のコードを実行できるとしています。当初、当該脆弱性は Apache Tomcat を Microsoft Windows 上で動作させていた場合、Microsoft Windows の特定の機能[ii]を悪用することにより攻撃が可能であると考えられていました。しかしながら、その後 Microsoft Windows 以外の OS 上で動作する Apache Tomcat においても、同様の脆弱性（CVE-2017-12617）が存在することが公表[iii]されました。これらの脆弱性については、一般社団法人 JPCERT コーディネーションセンターからも日本語での情報が公開[iv]されています。

警察庁においては、当該脆弱性を悪用する攻撃ツールや、これらの脆弱性に関する詳細な情報等が、既にインターネット上に公開されていることを確認しています。

2 Apache Tomcat の脆弱性（CVE-2017-12617）を標的としたアクセスの観測について

10 月 10 日 17 時以降、警察庁の定点観測システムにおいて、当該脆弱性を標的としたアクセスを観測しました（図1）。観測したアクセスは、脆弱性を悪用する HTTP PUT リクエストにより、特定の文字列を表示させる JSP ファイルのアップロードを試みるものであったことから（図2）、脆弱性の影響を受けるウェブサーバを探索する意図があるものと考えられます。当該アクセスにより脆弱性の影響を受けることが判明したウェブサーバに対しては、引き続き攻撃活動が実施される可能性が考えられます。

---

[i] http://tomcat.apache.org/security-7.html#Fixed_in_Apache_Tomcat_7.0.81

[ii] ファイルシステム NTFS の代替データストリーム（Alternate Data Stream）

[iii] http://tomcat.apache.org/security-9.html#Fixed_in_Apache_Tomcat_9.0.1
http://tomcat.apache.org/security-8.html#Fixed_in_Apache_Tomcat_8.5.23
http://tomcat.apache.org/security-8.html#Fixed_in_Apache_Tomcat_8.0.47
http://tomcat.apache.org/security-7.html#Fixed_in_Apache_Tomcat_7.0.82

[iv] 「Apache Tomcat における脆弱性に関する注意喚起」
https://www.jpcert.or.jp/at/2017/at170038.html

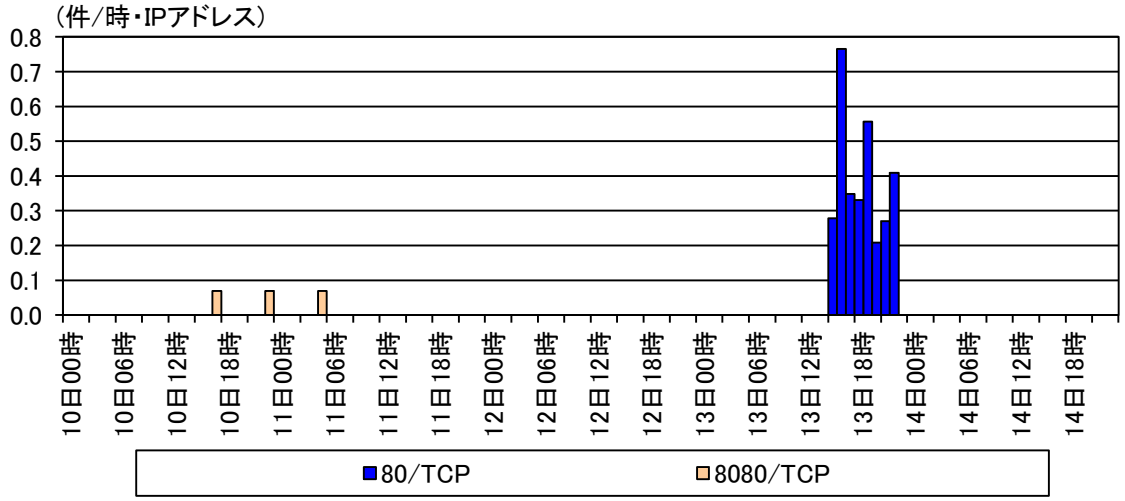

図1　Apache Tomcat の脆弱性（CVE-2017-12617）を標的としたアクセスの宛先ポート別件数の推移（H29.10.10～14）

```
PUT [redacted] HTTP/1.1
Host: [redacted]
Connection: keep-alive
Accept-Encoding: gzip, deflate
Accept: */*
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_10_1) AppleWebKit/
537.36 (KHTML, like Gecko) Chrome/39.0.2171.95 Safari/537.36
Content-Length: 50

<% out.println("AAAAAAAAAAAAAAAAAAAAAAAAAAAA");%>
```

図2　観測したアクセスのリクエスト内容（一部マスキングを実施）

3　推奨する対策

ウェブサーバの管理者等は、Apache Tomcat の使用有無及び使用していた場合にはバージョンの確認を実施してください。また、CVE-2017-12615 及び CVE-2017-12617 については、初期値で true となっている Apache Tomcat の readonly パラメータを false に変更し、HTTP PUT リクエストを有効にしている場合にのみ影響を受けることから、同パラメータの設定状況についても確認を実施してください。

使用している Apache Tomcat が影響を受けることが判明した場合には、開発元から公開されている以下の対策済みバージョンへアップデートを実施してください。

- Apache Tomcat 9.0.1
- Apache Tomcat 8.5.23
- Apache Tomcat 8.0.47
- Apache Tomcat 7.0.82

ただちにアップデートが困難な場合には、readonly パラメータを true へ変更し、HTTP PUT リクエストを無効にする暫定策も検討してください。

また、当該脆弱性に関する確認及び対策等を実施する際には、以下の事項にも留意してください。

- CVE-2017-12615 が Microsoft Windows 上で稼動している場合のみに影響を受ける脆弱性であったことから、対策は不要と判断していた場合であっても、再度 CVE-2017-12617 について確認及び対策等を実施してください。
- CVE-2017-12615 の対策済みバージョンとして公開された Apache Tomcat 7.0.81 については、CVE-2017-12617 の対策が実施されておらず、引き続き攻撃を受ける可能性が存在[i]します。
- 既に当該脆弱性が悪用された攻撃を受けている可能性も考えられるため、脆弱性が存在するバージョンの Apache Tomcat を利用していた場合には、ウェブサーバのログ、動作状況及び不審ファイルの有無等についても、併せて確認することを推奨します。

[i] 「Apache Tomcat に含まれる脆弱性(CVE-2017-12617)に関する脆弱性検証レポート」(NTT データ先端技術株式会社)
http://www.intellilink.co.jp/article/vulner/171004.html