NTTデータ・セキュリティ株式会社

Tomcat のディレクトリトラバーサルの脆弱性に関する検証レポート

2008/8/12
診断ビジネス部
辻 伸弘
松田 和之

【概要】

Tomcat において、文字エンコーディングの 1 つである UTF-8 のリクエスト処理、及び、シンボリックリンク処理に脆弱性が発見されました。この脆弱性により、ディレクトリトラバーサル攻撃を受ける危険性があります。
ディレクトリトラバーサル攻撃とは、相対パス（現在位置を基点として目的位置までのパスを示す記述方法）を利用して、管理者が意図しないディレクトリ・ファイルにアクセスする攻撃手法です。
想定される被害としては、悪意のあるユーザにより、Web サーバ上で公開されていないファイルへアクセスされ、機密情報が漏洩することが挙げられます。

この脆弱性は、Tomcat の、UTF-8 処理、及び、シンボリックリンク処理に欠陥があることに起因しています。これにより、UTF-8 を含む細工されたリクエストが送信されると、ディレクトリトラバーサル攻撃が可能となります。

今回、この脆弱性の再現性について検証を行いました。

【影響を受けるとされているシステム】

Apache Software Foundation Tomcat 6.0 ～ 6.0.16
Apache Software Foundation Tomcat 5.5 ～ 5.5.26
Apache Software Foundation Tomcat 4.1 ～ 4.1.37

【対策案】

このレポート作成現在（2008 年 8 月 12 日）、Tomcat 6.0 系のみ修正プログラムがリリースされており、5.5 系、及び、4.1 系については、修正プログラムはリリースされておりません。

この脆弱性は、Tomcat の設定内容に以下の 2 つの記述が存在する場合に影響を受けます。

① GET リクエスト送信時の文字エンコーディングに UTF-8 を利用している（URIEncoding=”UTF-8”）
② シンボリックリンクを有効にしている（allowLinking=”true”）

Tomcat の設定ファイル server.xml、及び、context.xml の設定状況を確認し、上記設定がされているかどうか確認してください。上記設定がされている場合、必要性の有無を確認し、不要であれば、無効にすることが暫定的な対策となります。

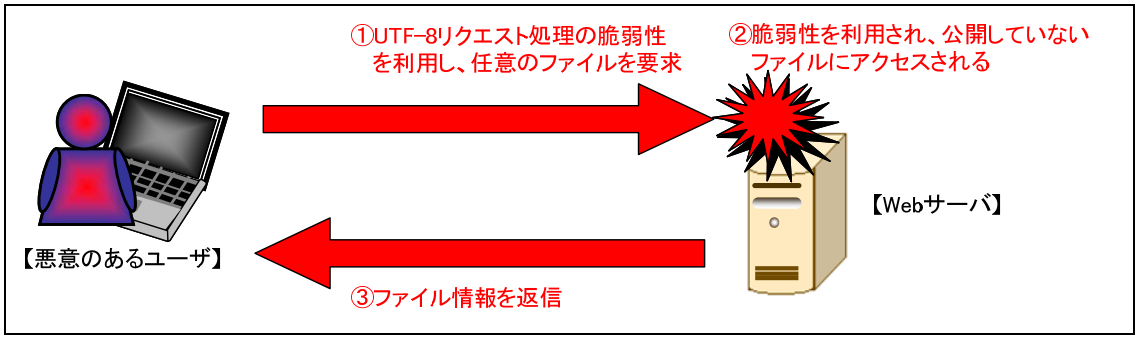
また、修正プログラムのリリース状況を確認し、正式な修正バージョンがリリースされた際には、速やかに最新版へアップデートすることが推奨されます。

【参考サイト】

Apache Tomcat - Apache Tomcat 6.x vulnerabilities
http://tomcat.apache.org/security-6.html

CVE-2008-2938
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-2938

【検証イメージ】



【検証ターゲットシステム】

Tomcat 5.5.26 がインストールされた CentOS 5

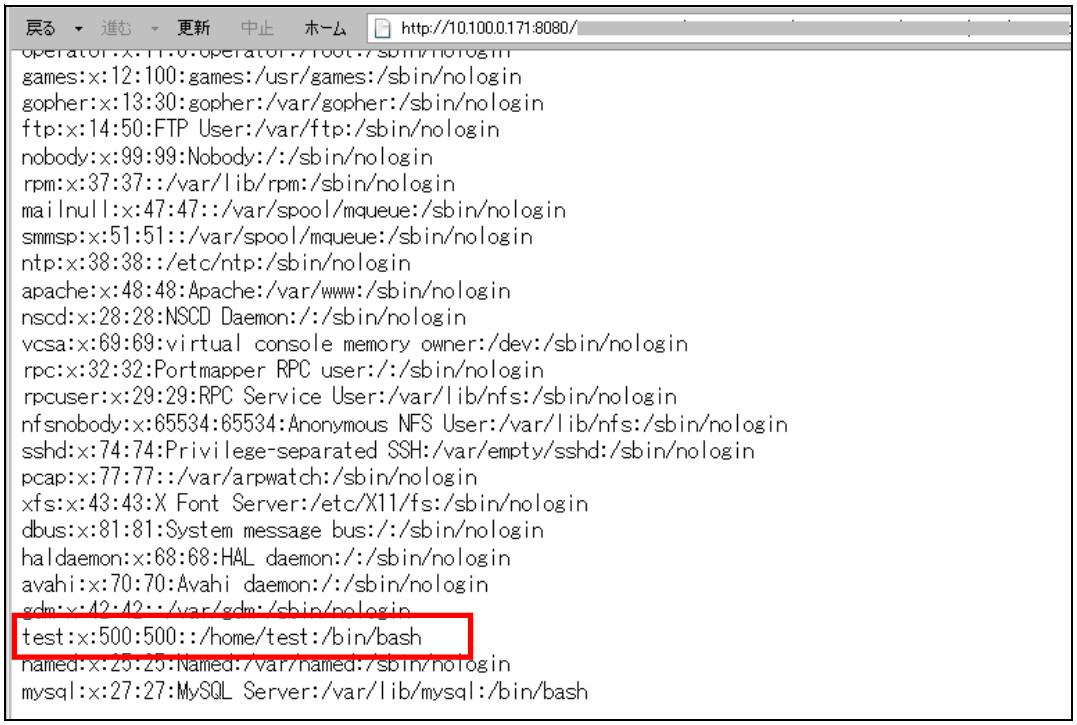
【検証概要】

ターゲットシステムに、細工した HTTP リクエストを送信することで、任意のファイルを読み出します。

【検証結果】

下図は、ディレクトリトラバーサルの脆弱性を利用し、ターゲットシステムのユーザ情報が格納されている「/etc/passwd」ファイルを、ブラウザから読み出した画面です。
赤線で囲われている部分に示すように、ターゲットシステムには、ユーザ名「test」が存在することがわかります。
これにより、悪意のあるユーザに、当該ユーザのパスワードクラックを行われ、システムへの侵入を許す危険性があります。

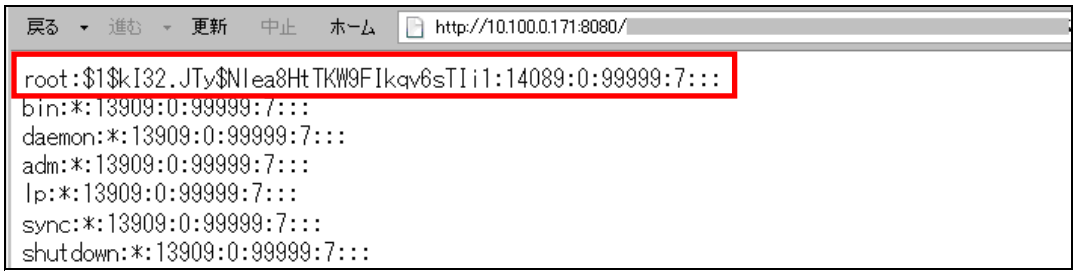
ターゲットシステムの/etc/passwd を読み出した画面



また、当脆弱性を利用することで、Tomcat の実行権限でファイルにアクセスすることが可能となります。つまり、Tomcat が管理者権限で稼動している場合、ターゲットシステムに存在する暗号化されたパスワードも読み出すことが可能となります。

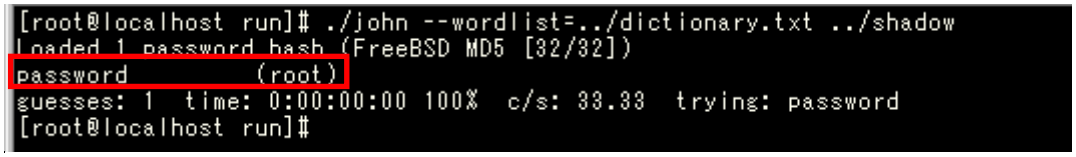
下図は、管理者権限で稼動している Tomcat に対して、脆弱性を利用し、暗号化されたパスワードが格納されている「/etc/shadow」ファイルをブラウザから読み出した画面です。
赤線で囲われている部分に示すように、ターゲットシステムの管理者権限ユーザ「root」の暗号化されたパスワードが閲覧可能な状態となっています。これにより、悪意のあるユーザに、暗号化されたパスワードからパスワードクラックを行われ、更なるシステムへの侵入を許す危険性があります。

ターゲットシステムの/etc/shadow を読み出した画面



下図は、取得した shadow ファイルをパスワード解析した結果画面です。このように、Tomcat が管理者権限で稼動している場合、悪意のあるユーザに、パスワード解析を行われ、更なるシステムへの侵入を許す危険性があります。

パスワードの解読画面



*各規格名、会社名、団体名は、各社の商標または登録商標です。

【お問合せ先】
NTT データ・セキュリティ株式会社
営業企画部
TEL:03-5425-1954
http://www.nttdata-sec.co.jp/