Security

Security updates

Please note that, except in rare circumstances, binary patches are not produced for individual vulnerabilities. To obtain the binary fix for a particular vulnerability you should upgrade to an Apache TomEE version where that vulnerability has been fixed.

Source patches, usually in the form of references to SVN commits, may be provided in either in a vulnerability announcement and/or the vulnerability details listed on these pages. These source patches may be used by users wishing to build their own local version of TomEE with just that security patch rather than upgrade.

The Apache Software Foundation takes a very active stance in eliminating security problems and denial of service attacks against Apache projects.

We strongly encourage folks to report such problems to the private security mailing list first, before disclosing them in a public forum.

Please note that the security mailing list should only be used for reporting undisclosed security vulnerabilities in Apache projects and managing the process of fixing such vulnerabilities. We cannot accept regular bug reports or other queries at this address. All mail sent to this address that does not relate to an undisclosed security problem will be ignored.

If you need to report a bug that isn't an undisclosed security vulnerability, please use the bug reporting system.

Questions about:

- how to configure TomEE securely
- if a vulnerability applies to your particular application
- obtaining further information on a published vulnerability
- availability of patches and/or new releases

should be addressed to the users mailing list.

The private security mailing address is: security (at) apache (dot) org

Note that all networked servers are subject to denial of service attacks, and we cannot promise magic workarounds to generic problems (such as a client streaming lots of data to your server, or re-requesting the same URL repeatedly). In general our philosophy is to avoid any attacks which can cause the server to consume resources in a non-linear relationship to the size of inputs.

Third-party projects

Apache is built with the following components. Please see the security advisories information for each component for more information on the security vulnerabilities and issues that may affect that component.

- Apache Tomcat 7.x: Tomcat 7 security advisories

- Apache OpenJPA
- Apache CXF: CXF Security Advisories
- Apache OpenWebBeans
- Apache MyFaces
- Apache Bean Validation

By default any regular TomEE releases uses latest sub project releases, so that we can follow all security fixes as much as possible.

Apache TomEE versioning details

As security is a key concern in many companies, TomEE team also considers to deliver specific security fixes for those external projects being fixed. For instance, if Tomcat fixes a security issue in Tomcat x.y.z, used in TomEE a.b.c, we will consider packaging a new security update release using the new Tomcat release.

In order to achieve a smoothly migration patch between a TomEE version and a security update, the TomEE team has decided to adopt the following versioning major.minor.patch[.security update]

- major ([0-9]+): it refers mainly to the Java EE version we implement. 1.x for Java EE 6 for example.
- minor ([0-9]+): contains features, bugfixes and security fixes (internal or third-party)
- patch ([0-9]+): only bugfixes applied

Optionally we can concatenate a security update to the version if TomEE source base if not impacted but only a dependency. Note this didn't happen yet.

Additional information

Secunia

Secunia is an international IT security company specialising in vulnerability management based in Copenhagen, Denmark.

There is an Apache Software Foundation vendor declared so you can follow all vulnerabilities related to Apache products. Of course, a Apache TomEE product is also available so you can search for know advisories.

Links

- http://apache.org/security/
- http://apache.org/security/projects.html
- http://apache.org/security/committers.html
- Common Vulnerabilities and Exposures database