JBoss Enterprise SOA Platform 4.3

Security HotFix Readme

RHSA-important: JBoss Enterprise SOA Platform security update

Abstract

This document contains important information and installation instructions regarding this security hotfix for the JBoss Enterprise SOA Platform.

This update has been rated as having important security impact by the Red Hat Security Response Team.

Four vulnerabilities have been discovered in the Tomcat server included in the 4.3 GA release of the JBoss Enterprise SOA Platform:

- A cross-site scripting vulnerability was discovered in the `HttpServletResponse.sendError()` method. A remote attacker could inject arbitrary web script or HTML via forged HTTP headers. (CVE-2008-1232)
- An additional cross-site scripting vulnerability was discovered in the host manager application. A remote attacker could inject arbitrary web script or HTML via the hostname parameter. (CVE-2008-1947)
- A traversal vulnerability was discovered when using a RequestDispatcher in combination with a servlet or JSP. A remote attacker could utilize a specially-crafted request parameter to access protected web resources. (CVE-2008-2370)
- An additional traversal vulnerability was discovered when the allowLinking and URIencoding settings were activated. A remote attacker could use a UTF-8-encoded request to extend their privileges and obtain local files accessible to the server process. (CVE-2008-2938)

All users are advised to run this patch to upgrade their JBoss Enterprise SOA Platform installation.

To run the patch type the following command, where ${as-installation-dir} is the dir where your SOA Platform server is installed:

```
java -jar SoaPatch.jar -x soa-4.3.0.SF1-patch.zip ${as-installation-dir}|
 tee patch.log 2>&1
```