

SAFETY FIRST: HOW RED HAT WORKS TO ENSURE THE SECURITY OF JBOSS ENTERPRISE MIDDLEWARE

1	THE RED HAT INDUSTRY-LEADING SECURITY RESPONSE PROCESS	3
2	LONG PRODUCT LIFECYCLE	3
3	INDEPENDENT THIRD-PARTY COLLABORATION ON SECURITY	4
4	KEY JBOSS ENTERPRISE MIDDLEWARE SECURITY FEATURES	5
5	BEST PRACTICES IN JBOSS ENTERPRISE MIDDLEWARE SECURITY	7
6	CONCLUSION	8



With security issues arising frequently in every layer of the open source software stack – the operating system, middleware, and application layers alike – security remains a top priority for enterprises. As an example, since 2009, more than 30 security issues were identified and resolved in Apache Web Server and Tomcat alone. Not surprisingly, 58 percent of large companies have open source security concerns.¹

Responding to open source security issues can be an arduous and time-consuming process. When a security issue is identified, businesses need to act quickly to protect themselves. Businesses first need to assess how critical a particular security issue is, and then determine whether it impacts them by checking if it applies to the versions of the software they are running. Because many businesses run multiple versions of open source software, investigating the impact of a security issue for even one layer of the software stack, such as the web server, can demand precious IT resources.

Red Hat® understands this. To relieve the burden from customers, Red Hat has integrated critical security features into JBoss® Enterprise Middleware and has created industry-leading processes and procedures to identify and mitigate any security issues that could arise. Red Hat supports customers' efforts to keep JBoss Enterprise Middleware-based applications secure for even the most mission-critical systems by helping them understand how all of the security issues, advisories, and support updates impact their environments.

Red Hat has integrated critical security features into JBoss Enterprise Middleware and has created industry-leading processes and procedures to identify and mitigate any security issues that could arise.

This whitepaper will describe:

- How the Red Hat security response mechanism has been designed to respond swiftly and effectively to security threats and vulnerabilities
- How the long-term product lifecycle of JBoss Enterprise Middleware products contributes to the security of Red Hat customers
- Key security features of Red Hat's foundational middleware solution, JBoss Enterprise Application Platform, and how each one contributes to overall security
- Best practices for businesses to follow to ensure the security of their applications

¹ Forrester Research: The State of Enterprise Software: 2009. June 2009.



THE RED HAT INDUSTRY-LEADING SECURITY RESPONSE PROCESS

One of the key differentiating factors and benefits of a JBoss Enterprise Middleware subscription is the Red Hat security response process.

Red Hat has a dedicated cross-functional team of security experts charged with driving rapid and effective responses to any and all security issues, whether they are identified by customers, the community, or other vendors. The Red Hat Security Response Team monitors and tracks issues and works with the various open source and Red Hat partner communities to address security concerns that impact Red Hat products, whether they were recently shipped, about to be shipped, or released several years ago. As a globally distributed team that provides 24/7 coverage to all Red Hat customers around the world, the Red Hat Security Response Team acts as the single point of contact for any business with security concerns about Red Hat products.

THE RED HAT SECURITY RESPONSE TEAM

- Acts as a central contact for all Red Hat security issues
- Spans Red Hat product lines, from platform to middleware solutions
- Tracks alerts and security issues within the open source and partner communities
- Investigates and addresses security issues in Red Hat products
- It is ideal that the copy here is long enough to occupy most of the sidebar.

LONG PRODUCT LIFECYCLE

Red Hat recognizes that upgrading software for business applications can be a painful and costly process for enterprises. To alleviate this process, all Red Hat enterprise software products possess extended product support lifecycles (e.g., seven years for JBoss Enterprise Application Platform), during which Red Hat issues security alerts and patches for all significant identified issues. These lifecycles break down into three phases: full support, transition support, and maintenance support.

No matter which lifecycle phase a product currently falls into, critical security issues are addressed asynchronously to maximize security for users of that product. That is, Red Hat publishes critical fixes as soon as they are identified. For issues that are less severe, fixes are released in the next update of the product. During transition or maintenance phases, when updates are less frequent, Red Hat issues security advisories as needed (see Figure 1).



Safety first: How Red Hat works to ensure the security of JBoss Enterprise Middleware

FIGURE 1: EXAMPLE OF THE PRODUCT LIFECYCLE OF JBOSS ENTERPRISE APPLICATION PLATFORM

7 Year Long-term Product Lifecycle			
	Full Support	Transition	Maintenance
Duration	4 years	1 years	2 years
Update Frequency	Quarterly Target	Updates released as needed	Released as needed
Update Form	Minor Releases	Minor Releases	Critical Patch Releases
Update Content	Defects, security issues, non-intrusive features	Defects, security issues, non-intrusive features	Critical defects and security issues
Critical Security Issues	Released asynchronously	Released asynchronously	Released asynchronously

Long-term product lifecycle that maintains application compatibility; all fixes are committed upstream first.

Red Hat commits security fixes to community projects before they are released publicly so that software remains compatible throughout the lifecycles of both community and enterprise projects. Typically, advisories are not published until Red Hat has a fix that mitigates the identified security problem to avoid giving anyone a chance to exploit a given vulnerability. All advisories come bundled with their fixes.

To find out if a particular issue affects them, customers simply enter the issue's Common Vulnerability and Errors (CVE) ID number into the Red Hat website to get the advisories and fixes that impact their particular installed release. They can also query the vulnerability from the National Vulnerability Database, which shows all Red Hat patches related to a particular issue.

Red Hat also reassures businesses when a security issue or vulnerability does not impact them. This knowledge is as vital for managing mission-critical applications as the knowledge of what does impact them. By leveraging Red Hat's security response process, customers save valuable time they would otherwise have to spend determining if a given issue impacts their environments.

INDEPENDENT THIRD-PARTY COLLABORATION ON SECURITY

Red Hat also works with a broad range of vendors whose products impact Red Hat products and vice versa. After all, vulnerability in another layer of the application stack can have profound implications for JBoss Enterprise Middleware-based applications. For example, most businesses that use Java virtual machines have experienced security issues. Red Hat routinely works with the vendors of those products to ensure that any security issues related to any of the Java virtual machines included in the Red Hat suite of products are quickly addressed.

Red Hat also works closely with independent third-party security evaluators and agencies to verify that a specific version of a Red Hat product meets industry security standards, including Common Criteria. Red Hat solutions that achieve Common Criteria certification, including JBoss Enterprise Application Platform and Red Hat Enterprise Linux, have undergone a thorough, independent security review.



WHAT IS COMMON CRITERIA?

Businesses in industries that require significant security assurance, including financial services, healthcare, and government agencies, rely on Common Criteria certifications to provide confidence that evaluated IT solutions comply with widely-accepted security standards. Common Criteria is a set of internationally approved criteria for evaluating and certifying the information security of IT products and information systems, and is currently recognized in 25 countries. Security evaluations based on Common Criteria assess the security performance and reliability of the target system. These factors are tested and validated by an accredited, third-party source against the Common Criteria Standard for Information Technology Security Evaluation (ISO/IEC 15408).

RED HAT SOLUTION	TARGET COMMON CRITERIA EVALUATION ASSURANCE LEVEL (EAL)
JBoss Enterprise Application Platform 5	EAL 4+
JBoss Enterprise Application Platform 4.3	EAL 2+
Red Hat Enterprise Linux 5	EAL 4+

KEY JBOSS ENTERPRISE MIDDLEWARE SECURITY FEATURES

In addition to these security processes and procedures, Red Hat has embedded—and is continually adding and enhancing—features that allow customers to feel confident enough in the software to use it to build even their most mission-critical applications. Many of these features are built into Red Hat's foundational Java™ Enterprise Edition (Java EE) middleware solution, JBoss Enterprise Application Platform. Since JBoss Enterprise Application Platform is included in all other JBoss Enterprise Middleware solutions, each JBoss product benefits from these security features, which include:

- **Authorization framework for Enterprise Java Beans (EJB) and web applications.** This framework gives businesses plug-and-play access control mechanisms for their Java EE applications. As part of this framework, JBoss Enterprise Application Platform supports OASIS XACML V2-compliant engines that enable context-driven authorizations in addition to role-based access control. And because the XACML engine is provided natively in JBoss Enterprise Application Platform, it is easy to deploy for business applications.

Red Hat created this authorization framework because Java EE provides only coarse-grained access control to applications. However, businesses often need to leverage context-driven authorization as well. The context-driven authorization included in JBoss Enterprise Application Platform provides advanced security functionality, such as the ability to allow access to a particular URL only between certain hours or to prohibit certain employees from performing transactions over a specified dollar threshold. This allows businesses to offload access control rules from their business applications, thus reducing application overhead and improving performance. Customers can also extend JBoss Enterprise Application Platform's authorization framework with their own custom authorization modules.



- **Negotiation support for web applications.** This popular feature is most commonly used when end users need to log on to a Kerberos-backed desktop, such as Windows desktop (backed by Active Directory), and access JBoss-based web applications with a seamless and secure single sign-on procedure.

The way this works: the browser transmits desktop login information to the container on the web application platform and to Active Directory. Any Kerberos service can act as the anchor for enabling the access. This uses a Red Hat technology called JBoss Negotiation that has been integrated into the JBoss platform as a toolkit to help system administrators set up this feature.

- **Security audit feature for EJB and web applications.** For businesses concerned about meeting regulatory compliance, Red Hat offers an audit framework for JBoss Enterprise Middleware that is enabled for both web and EJB applications, and which captures all security events for both types of applications. Red Hat recommends using container security. It is important to understand that if container security is disabled for the web by a business (so it can do its own authentication and access control), then the audit feature cannot be enabled as a default.

The audit feature provides a log that details what each user has accessed, what routes they came in through, any exceptions that came in, and the entire audit trail along the way. For sensitive information such as cookies, Red Hat provides a secure way to mask aspects of the audit to protect the underlying information. However, since this audit feature is performance intensive, it is not deployed by default—system administrators have to explicitly enable it.

- **Password masking for configuration files.** The latest version of each JBoss Enterprise Middleware solution is based on the JBoss Microcontainer. Within this microcontainer, services and configuration files are treated as microcontainer beans. To secure these beans, users can take advantage of the password masking feature to ensure these configuration files remain secure and protected. The password masking feature can also be used for popular middleware interfaces, such as Tomcat connectors and data sources. With the help of this feature, Red Hat customers can take the necessary steps toward centralized password management for their application environments.



BEST PRACTICES IN JBOSS ENTERPRISE MIDDLEWARE SECURITY

Although Red Hat has put all of these processes, procedures, and product features in place to protect JBoss Enterprise Middleware customers, businesses should still follow best practices for ensuring their applications are made as secure as possible. Here are some best practices for achieving this:

- **Choose a secure environment.** When given the option of implementing a certified versus non-certified open source product or platform, businesses should choose certified. Certifications by independent third parties provide an extra layer of assurance that software is secure enough to deploy for mission-critical applications. For example, many Red Hat products undergo the Common Criteria certification, where independent third parties examine Red Hat's development procedures, source code, design documents, and test suites for security vulnerabilities.
- **Update your software and apply patches as they become available.** Keeping software updated and patched based on the latest security advisories and fixes is an essential part of securing any enterprise application. By keeping an environment up-to-date, users can help avoid the legal, privacy, reputation, and financial risks associated with security breaches.
- **Enable auditing.** Businesses have the option of enabling auditing within a JBoss Enterprise Middleware platform, primarily for authentication. By keeping tabs on who is coming into the systems and what they are doing, businesses can help keep their applications secure. If issues do occur, audit logs serve as one of the most valuable tools in security investigations.
- **Implement secure configurations.** JBoss Enterprise Middleware platforms leverage the concept of security domains. Businesses can configure their certification login modules in a way that plays a role in the security of their applications. As a best practice, Red Hat recommends using the Dynamic Login MBeans Service, which allows businesses to define their security domain configurations as part of their deployments.
- **Encrypt passwords.** Red Hat provides a number of opportunities for businesses to encrypt and hash passwords when the data source is either the JBoss login module or Tomcat connector module. An important best practice is to take advantage of these opportunities to bolster other authentication methods being used.



CONCLUSION

Keeping applications secure is a top priority for businesses.

As the world's leading provider of open source solutions, Red Hat understands the importance of security. Through its robust security mechanisms, Red Hat gives customers across its entire enterprise product portfolio—from Red Hat Enterprise Linux to each JBoss Enterprise Middleware platform—critical help addressing security issues and vulnerabilities. With its industry-recognized Red Hat security response processes, its commitment to delivering security fixes throughout a long-term product lifecycle, the key security features incorporated within the products themselves, and advice offered on best security practices, Red Hat makes it possible for its open source solutions, including JBoss Enterprise Middleware, to be a trusted foundation for even the most mission-critical applications.

RED HAT SALES AND INQUIRIES

NORTH AMERICA
1-888-REDHAT1
www.redhat.com

**EUROPE, MIDDLE EAST
AND AFRICA**
00800 7334 2835
www.europe.redhat.com
europe@redhat.com

ASIA PACIFIC
+65 6490 4200
www.apac.redhat.com
apac@redhat.com

LATIN AMERICA
+54 11 4341 6200
www.latam.redhat.com
info-latam@redhat.com