Securing Java Applications

Joseph Konieczka

BrixBits Sales Engineer

Agenda

- Current State
- Resources
- Top 10 Vulnerabilities
- BrixBits Security Analyzer
- Q & A

Questions to ask yourself

- How often do you review your code for vulnerabilities?
- When do you normally deploy the quarterly critical patches?
- How often do you review the patch Risk Matrix?
- When was the last time auditors evaluated your coding practices?

What does a data breach cost?

- Cost per stolen record $154
- Cost of the breach $3.79 million
- 23% increase in total cost of since 2013
- 12% percent increase in per capita cost since 2013
- Likelihood of a breach 22%
- 2015 Cost of Data Breach Study: Global Analysis http://www-03.ibm.com/security/data-breach/

Java Vulnerabilities timeline

- Historically near the top of the list with a slight lull in 2014
- 2015 – Java back on most wanted list
- https://heimdalsecurity.com/blog/java-biggest-security-hole-your-computer/

NATO hacked by Russian Pawn Storm hackers

- CVE-2015-4902 and CVE-2015-2590 patches addressed click to play and malware download vulnerabilities
- http://www.infoworld.com/article/2995088/security/oracle-slams-door-on-russian-cyber-spies-who-hacked-nato-pcs-through-java.html

OWASP Top 10 2013 Application Security Flaws

- Injection
- Broken Authentication and Session Management
- Cross-Site Scripting (XSS)
- Insecure Direct Object References
- Security Misconfiguration
- Sensitive Data Exposure
- Missing Function Level Access Control
- Cross-Site Request Forgery (CSRF)
- Using Components with Known Vulnerabilities
- Unvalidated Redirects and Forwards

https://www.owasp.org/index.php/Top10#OWASP_Top_10_for_2013

OWASP

- Open Web Application Security Project (OWASP)
  - https://www.owasp.org/index.php/Main_Page
- Austin Chapter
  - https://www.owasp.org/index.php/Austin
- Top 10 Project
  - https://www.owasp.org/index.php/Top_10

OWASP Java Resources

- https://www.owasp.org/index.php/Java_Security_Resources
- https://www.owasp.org/index.php/Category:OWASP_Java_Project
- https://www.owasp.org/images/8/89/OWASP_Top_10_2007_for_JEE.pdf
- http://www.slideshare.net/MasoudKalali/owasp-top-10-and-java-ee-security-in-practice

Coding Guidelines

- Oracle
  - Secure Coding Guidelines
    - http://www.oracle.com/technetwork/java/seccodeguide-139067.html
  - Java Security Resource Center
    - http://www.oracle.com/technetwork/java/javase/overview/security-2043272.html
- SEI CERT Oracle Coding Standard for Java
  - https://www.securecoding.cert.org/confluence/display/java/SEI+CERT+Oracle+Coding+Standard+for+Java

Standards

- National Vulnerability Database Common Vulnerability Scoring System [CVSS]
  - https://nvd.nist.gov/cvss.cfm
- PCI SSC Data Security Standards Overview
  - https://www.pcisecuritystandards.org/security_standards/
  - Requirement 6: Develop and maintain secure systems and applications

Books - Slightly dated

- Java Coding Guidelines: 75 Recommendations for Reliable and Secure Programs
- CERT Oracle Secure Coding Standard for Java
- Authors of both books: Fred Long, Dhruv Mohindra, Robert C. Seacord, Dean F. Sutherland, David Svoboda

Training & Certification

- SANS
  - DEV541: Secure Coding in Java/JEE: Developing Defensible Applications
  - https://www.sans.org/selfstudy/course/secure-coding-java-jee-developing-defensible-applications
- GIAC Secure Software Programmer-Java (GSSP-JAVA)
  - http://www.giac.org/certification/secure-software-programmer-java-gssp-java

About Our Agents

- Collect critical information needed to ensure that Java applications are running efficiently and securely
- Architected to be run stand-alone or be easily integrated into existing infrastructure
- Focused on reporting, events, and notifications
- Run as an embedded agent within the Java runtime
- Most can be run on-demand – only when needed

Security Analyzer Product Highlights

- Capture all Java security exceptions
- Identify application configuration risks, compliance and changes
- Track permission use and admin activity
- Integrates with existing SIEM
- Runtime Application Self Protection (RASP)
- Notification of security events
- Verify the security of 3rd party or outsourced code and applications

Agent Overview

Agent	Description	Active/On-Demand
Socket Analyzer	Monitor network endpoints for activity, performance, errors	Active
Security Analyzer	Detect and log all security exceptions and extend native Java security	Active
End User Experience	Monitors front end page load times and measures application server responsiveness and availability	Active
Response Analyzer	Discover commonly used code paths and stall points that can cause Java application performance issues	On-Demand
Quality Analyzer	Catch all runtime exceptions and report on Java application quality	On-Demand
Memory Detective	Monitor and alert on JVM memory use and leaks	On-Demand
Health Monitor	Monitor overall runtime health to easily diagnose performance issues	Active
Lock Detective	Find and report on application lock contention issues	On-Demand
Log Notification Engine	Configure notifications for Java application server log errors	Active
Agent Manager	Manage Java agents	Active

Call to action

- Stay informed
- Log vulnerabilities (security defects) in your bug tracking system
- Consider certification
- Spread the word
  - Other developers
  - Systems administrators
  - Business teams


Q&A

http://brixbits.com/