Security Process and Procedure Changes after Acquisition

Bruce Lowenthal – Director, Oracle Security Alerts Group

Agenda

- Acquisitions
- Key points
- Defect process differences for security vulnerabilities
- Oracle security programs
- Acquisition policy/procedure adoption and issues
- Summary

In this presentation, security defects means those defects that result in security vulnerabilities

Oracle Technology Acquisitions

- Occur frequently – about 1 per month for last 5 years
- Customers expect same security standards as Oracle
- Acquisitions get a big, red bull’s eye

Oracle Technology Acquisitions

- Most acquisitions need major program enhancements
  - Testing and training; development awareness
  - Security versus non-security bug handling
- All need migration to Oracle policies and procedures

Key Points for this Presentation

- Process/policies for security bugs differs from other bugs
  - Employees need to know that security is very important
  - Programs must stress quick fix deployment by customers
  - Security defects require enhanced policies, processes & organization
  - Need to develop product security experts
  - Need to enhance product testing for security bugs

Process/Policy Differences for Security Defects

Overview

- Support and Development organizations
  - Need special organization to address security defects
  - Will only discuss development organization in this presentation
- Process flow for security bugs differs from other bugs
- Access to security bug reports highly restrictive
  - “Need to know” only
  - Hierarchical access restrictions to security bug reports
    - Development only has access
    - By product suite, product group, product or product component
  - <1% of developers can access any particular security bug report
  - Helps to reinforce that security bugs are special

Organization of Development Security Personnel for Product Security Vulnerabilities

- Hierarchy
  - Global Product Security – all products
  - Security Leads – business units
  - Security points of contact – products or product components
  - Individual contributors: developers, QA, product management, etc.
- People higher in the hierarchy
  - Have more training and experience; are consultants for others
  - Review security fixes for security and non-security issues
  - Are tasked to “get out the word” and manage security projects

Security Leads and Security points of contact are named during the first 100 days after an acquisition

Organization of Security Personnel
Benefits or Hierarchy

- Oversight organization improves product security
- Consulting “services” are in great demand
  - e.g. What is the defense for CSRF? (What is CSRF?)
- Security bug reviews are very effective
  - Probably ¼ of fixes are rejected
- Fosters global programs such as automated testing
- Creates secure coding standards and other documents
  - Leverage expertise of 100’s of security experts
  - Referenced for proper tactical and strategic fixes

Externally Discovered Defect Handling Process for non-security defects

- Only customer defect reports are eligible
- Standard sustaining engineering policies
  - Fix quickly, get fixes to reporting customer quickly, move on
  - Review fix but no comprehensive regression testing
  - Fix in main code line and then in customer version-platform only
  - Do the minimum to satisfy reporter – no further investigations
  - Comprehensive testing when next version is released

Baseline support for non-security product defects is standard sustaining engineering model

Externally Discovered Defect Handling Process for Security defects

- Input from customers, researchers and public disclosures
- Fix security defect and “nearby” security bugs
- Fix all version-platform combinations (60+ for Database)
- Extended testing and extra review by security specialists
  - Belief: More testing leads to faster customer fix application
  - Quality delivery takes time but leads to faster adoption
  - Comprehensive testing of applications with full stack
- May trigger additional “projects”

Security defect handling process differs from non-security defect process

Oracle Security Programs

- Training
- Testing
- Certification – not covered in this presentation
- Remediation
  - Fix distribution
  - Disclosure policies

As acquired technologies adopt corporate programs, a number of issues surface

Oracle Security Programs

Training

- All developers, QA, et al. take corporate security training
  - Focus is culture change: “Security is Important”
  - Compliance reviewed by President on regular basis
- Job specific training and training materials
  - Secure coding standards for development
  - Checklists for reviewers
  - Outside education for internal penetration testers, etc.
- Job specific policies, processes and procedures
  - General process flow for handling security bugs
  - Oracle is serious about confidentiality – less than 1% rule
  - Customer is key

Oracle Security Programs

Testing and Reviewing

- Traditional testing and reviews enhanced for security
  - Traditional: Functional, failure, stress testing and reviews
  - Enhanced: Specialist reviewers, tests backported to old releases
- External to group testing and reviewing
  - Internal specialist reviewers for vulnerability fixes
  - Oracle penetration test and review (Ethical Hackers)
  - Outside Oracle penetration test and reviews
- Extensive use of automated tools
  - Internally developed tools specific to Oracle
  - Externally developed tools
  - Continuous research for new automated tool candidates

Oracle Security Programs

Remediation

- Definition: Post release vulnerabilities fixing
- Reporting sources: Internal, customer and researcher
- At Oracle
  - 3% Researcher reported via secalert_us@oracle.com
  - 10% Customer reported via normal Customer Support
  - 87% Internally discovered, especially by automated testing
  - Acquired technologies often differ significantly
- Delivery and documentation
  - Critical Patch Updates – delivered quarterly
  - Security Alerts – non-scheduled emergency distributions
  - Bulletin boards – pass through products

Oracle Security Programs
Remediation and Researchers

- Program for addressing researcher security bug reports
- Goals
  - Two working days to acknowledge report submission
  - Ten working day to confirm report of a security bug
  - Fix delivery times vary
    - Oracle DB delivers on 60+ version-platform combinations
    - Often include comprehensive coverage of “nearby” vulnerabilities
- Monthly status reports provided until resolution
- Researchers acknowledged in public documentation

Good relationships with researchers is important. Make it attractive for researchers to submit security bugs

Security Programs Integration with Acquisitions

- Acquisitions with minimal or no security programs
- Acquisitions with security programs
- Comment and summary

Acquisitions with Minimal or No Security programs

- Most acquisitions have minimal or no security programs
- Security defects handled like non-security defects
  - No security specialist to consulting and review
  - No special disclosure rules
  - No special testing requirements
- “100 day plan” addresses security program adoption
  - Security Leads and security points of contact named
  - Many deliverables are plans
  - Completion “pushed” by Global Product Security

Acquisitions rarely have significantly different processes for handling security bug versus non-security bugs

Acquisitions with Minimal or No Security programs

- Most are startled by security programs
  - Training
  - Testing
  - Remediation
- Many are surprised by “interest” from Researchers
  - Oracle brand makes them a target
  - Need staff/process for Researcher communication
  - Tracking and most communication by Global Product Security

Acquisitions with Minimal or No Security programs

Training

- All developers, QA and PM take global security course
  - Compliance tracked by Global Product Security and reviewed by President on a regular basis
  - Promotes awareness that Oracle is serious
  - Security considered a key value of Oracle branding
- Special training for Security Leads & Points of Contact
  - Group meetings at headquarters
  - Weekly calls for Security Leads
  - Newsletters, bulletins, etc.
- Technology specific training encouraged

Acquisitions with Minimal or No Security programs

Testing

- Automated testing started (or enhanced)
  - Internally and externally developed tools
  - Often very welcome by acquired groups
  - Usually requires considerable resources to become effective
- Products often added to full stack testing suites
  - Applications plus full stack infrastructure
  - **Comprehensive testing is key to rapid customer fix deployment**
- For time critical technology security issues
  - Internal penetration testing
  - Oracle is considering quick result “testing services”

Acquisitions with Minimal or No Security programs

Remediation

- Build infrastructure for researcher communication
  - Global Product Security communicates with researchers
  - Security points of contact assigned
- Migrate to corporate tracking tools, policies & procedures
  - Internal and external disclosures policies
    - Few can view security bugs (< 1% rule)
    - No special customers
  - Internal to group specialists for reviews and communication
  - Global Product Security specialists for reviews and consultation

Acquisitions with Minimal or No Security programs

Remediation Issues

- Non-security bugs handled differently than security bugs
  - Fix “nearby” vulnerabilities, more comprehensive testing
- Internal disclosure issues
  - Disclosure only via advisories plus need to know (< 1% rule)
  - Need to know does not include Customer Support
- External disclosure issues
  - Customer disclosure information limited to advisories
  - No special customers

Recognition that non-security bugs are handled differently from security bugs is key to security fix quality

Acquisitions with Significant Security programs

- Most are not as extensive as Oracle’s
  - Testing
  - Remediation
- Policy and procedures often clash
  - Internal/External disclosure policies
  - Fix distribution model (quarterly versus immediate)
- Some are surprised by “interest” from Researchers
  - Oracle brand makes products a more interesting target

Acquisitions with Security programs
Testing

- Few perform as much automated testing as Oracle
  - Oracle can almost always help with site licenses, etc.
  - Many automated tests highly effective
  - Depending on tool, significant resources are required after site license for false positives, etc. but at least license is not a barrier
- Few perform as much defect fix testing as Oracle
  - Regressions often more of a barrier than at Oracle
  - Full stack + application tests take six weeks

More thorough regression testing seems to result in faster customer patch application

Acquisitions with Security programs
Remediation

- Researcher communication usually easily migrated
- Fix strategy may need to be upgraded especially where Sustaining Engineering fixes security vulnerabilities
  - Non security fix: Do the minimum to get customer going
  - Security fix: Fix nearby vulnerabilities; consider projects
- Bug tracking infrastructure migrated
- Disclosure and release policies migrated

When security bug fixes are released, “nearby” bugs are often immediately attacked

Acquisitions with Security programs
Remediation Issues

- When bug tracking infrastructure is not quickly migrated
  - Global Product Security has difficulty monitoring
  - Too often, security handling falls short of internal standards
  - Probably one of the biggest issues
- Disclosure and release policies need to be migrated
  - Issues with customers
  - Changing to new fix delivery vehicles can result in disruptions
    - Some technologies were moving to Oracle’s model anyway (Scheduled releases, with comprehensive testing)

Lack of common bug tracking infrastructure has resulted in sub-standard security

Summary

- A comprehensive program to address security defects is key for brand value
- Acquired technologies often fall short
  - Employees need to know that security is very important
  - Programs must stress quick fix deployment by customers
  - Security defects require enhanced policies and processes
  - Need to develop product security experts
  - Need to enhance product testing for security defects

Comment: While Oracle acquired products may need to quickly adopt enhanced processes now, all public products will need to address similar processes soon