ORACLE®

OpenWorld 2017 THT7571: The Security Benefit of Premier Support

ORACLE OPEN WORLD

October 1–5, 2017
SAN FRANCISCO, CA

Reshma Banerjee
Director
Security Alerts Group
Global Product Security
October 4, 2017

ORACLE

Program Agenda

1. What is Oracle Software Security Assurance?
2. Why/How does Oracle release security fixes?
3. Can you do away with Oracle fixes?
4. Any business implications of running vulnerable systems?
5. What should you do?

What is Oracle Software Security Assurance?

Encompassing every phase of the product development lifecycle, Oracle Software Security Assurance (OSSA) is Oracle's methodology for building security into the design, build, testing, and maintenance of its products.

Oracle's goal is to ensure that Oracle's products, as well as the customer systems that leverage those products, remain as secure as possible

https://www.oracle.com/support/assurance/index.html

- OSSA programs include:
  - Critical Patch Update and Security Alert Programs
  - “Secure by default” initiative
  - Secure Coding Standards
  - Security certifications (Common Criteria and FIPS)
  - Ethical hacking
- OSSA applies to:
  - Oracle on-premises products
  - Oracle cloud products and services

What is ongoing security assurance?

- The primary objective:
  - To help ensure that security controls provided by software are effective, work in a predictable fashion, and are appropriate for that software and
  - To make sure that this objective continues to be met over time (throughout the useful life of software)
- As part of its commitment to ongoing assurance,
  - Oracle periodically releases security fixes and
  - Continuously introduces security enhancements in its products

Why does Oracle release security fixes?

- To address security defects (i.e., “vulnerabilities) in Oracle code
- To address security vulnerabilities in third-party components embedded in Oracle product distributions e.g. Heartbleed
- To maintain a product’s security posture (e.g., removal of obsolete crypto for use of stronger algorithms)
- To address new attack vectors (or new classes of vulnerabilities)
- To provide better “security in depth”

How does Oracle release security fixes?

- Critical Patch Updates are released quarterly (for all Oracle on-premises products) on a predictable schedule
- Off-cycle Security Alert Advisories are released for high-risk vulnerabilities
- Oracle fixes highest security bugs first
- Security bugs are tested across the stack to prevent regression issues
- Critical Patch Update and Security Alert fixes are only provided for product versions that are "covered under the Premier Support or Extended Support phases of the Lifetime Support Policy."

https://www.oracle.com/support/assurance/vulnerability-remediation/introduction.html

How “critical” are the fixes in the Critical Patch Update?

- ‘C’ in CPU stands for CRITICAL
- Many of these bugs, if successfully exploited, can result in serious compromise for the affected Oracle system(s)
- **Oracle continues to receive reports of successful exploitation of vulnerabilities for which Oracle has already released fixes.**

https://www.oracle.com/technetwork/topics/security/alerts-086861.html

Can you do away with Oracle security fixes?

Can a firewall (or other mitigation measures) protect you?

- NO!
- Generally, if a bug is “remotely exploitable without authentication” and the affected interface is visible in the network, the bug can be exploited
- Historically, Oracle has found that mitigation published by non-Oracle sources (other than "apply the patch“) has often been ineffective or has caused adverse side effects leading to application failures
- Security companies (vendors of firewall, IDS, IPS, SIM, etc.) do not get “special” information from Oracle. They do not have the technical ability or knowledge required to develop attack signatures that could detect or much less prevent attempts of exploiting Oracle vulnerabilities

Can you do away with Oracle security fixes?

Can lack of patching degrade your security posture over time?

- YES!
- CPU fixes are being reverse-engineered by malicious actors to identify the nature of the bug and develop weaponized version of the exploit (e.g., Metasploit, a free penetration testing tool)
  - Note: Hacking technology is being “continuously improved”
- Malicious actors (and security auditors) know that many customers will not apply security patches in a timely fashion
- This also means that malicious actors are further empowered after the release of each Critical Patch Update to carry attacks against customers who do not apply the Critical Patch Update

Can you do away with Oracle security fixes?

Are there business implications of running vulnerable systems?

- YES!
- Failure to apply security fixes severely degrades security over time
  - Exploits for vulnerabilities are included in increasing numbers of "Hacker Exploit Kits
  - Impact of successful exploits is not contained due to lack of inclusion of in-depth fixes
  - Customers should assume that product versions that are no longer supported have nearly all the vulnerabilities in newer versions plus more
- Good IT governance demands applying published security fixes in a timely manner
- Lack of timely security patching could have statutory compliance implications and give rise to regulatory enforcement actions

What should you do?

- Keep up with security releases!
  - Critical Patch Updates and Security Alerts
- Subscribe to Oracle’s security notifications
  - https://www.oracle.com/technetwork/topics/security/securityemail-090378.html
- Stay on supported releases
  - Later releases provide an enhanced security posture
  - Follow Oracle’s security guidelines
- Assess the security assurance practices of your vendors
  - And leverage the programs that are relevant to you!

For more information

- Oracle Software Security Assurance web site
  - https://www.oracle.com/support/assurance/index.html
- Security Alerts and Critical Patch Updates
  - https://www.oracle.com/technetwork/topics/security/alerts-086861.html
- Lifetime Support Policy
  - http://www.oracle.com/us/support/lifetime-support/index.html

Questions?

ORACLE®