
ORACLE®

CON6302: To Patch or Not to Patch Answering the CPU Question

Bruce Lowenthal
Senior Director
Oracle Security Alerts Group

Juan Perez-Etchegoyen
CTO
Onapsis

ORACLE OPEN WORLD

ORACLE

onapsis

Timeline of a 2017 Compromise

- Timeline of a 2017 compromise
  - March: Struts 2 CVSS 10 fix released for CVE-2017-5638
  - Mid May-July end: Equifax hacked, 143 Million Americans compromised
  - September: Public Announcement, CEO called to testify before Congress, CIO and CSO retire
  - Equifax criticized for not applying fixes quickly enough

- How does one determine how quickly Oracle fixes should be applied?
  - Should special care be given to mission-critical applications?

Business-Critical Applications

Why should we care about securing these applications?

Business-Critical Applications store and process the most critical business information in the Organization. If these applications are breached, an intruder would be able to perform different attacks such as:

- **ESPIONAGE**: Obtain customers/vendors/human resources data, financial planning information, balances, profits, sales information, manufacturing recipes, etc.
- **SABOTAGE**: Paralyze the operation of the organization by shutting down the system, disrupting interfaces with other systems and deleting critical information, etc.
- **FRAUD**: Modify financial information, tamper sales and purchase orders, create new vendors, modify vendor bank account numbers, etc.

Business-Critical Applications

What defines them?

- Big deployments with multiple servers
- Proprietary components and protocols
- Heavily integrated applications
- Strong customizations layer
- Complex configurations
- Critical business processes
- Strict change management processes
- Typically running on-premise

Some examples:

- Oracle E-Business Suite
- Oracle JD Edwards
- Oracle Peoplesoft
- Oracle Fusion Applications

Business-Critical Applications

Why are these applications different?

- Proprietary protocols and components
  - JDENET, PeopleTools, T3, Oracle Forms, NodeManager…
- Strong customization layer
  - E1JETDev, OMW (Oracle Management Workbench), OAF (Oracle Applications Framework), Siebel Query Language, Oracle ADF/JSF (Fusion)
- Heavily integrated applications
  - EBS: Oracle Open interface, Concurrent Program, Java™ Service, XML Gateway, PL/SQL API
  - JDE: Z Tables, Business Interfaces, JDENET
  - Fusion: Oracle Enterprise Repository (ADF Services, SOA, Business Events)

Business-Critical Applications

Traditional Approach to securing them

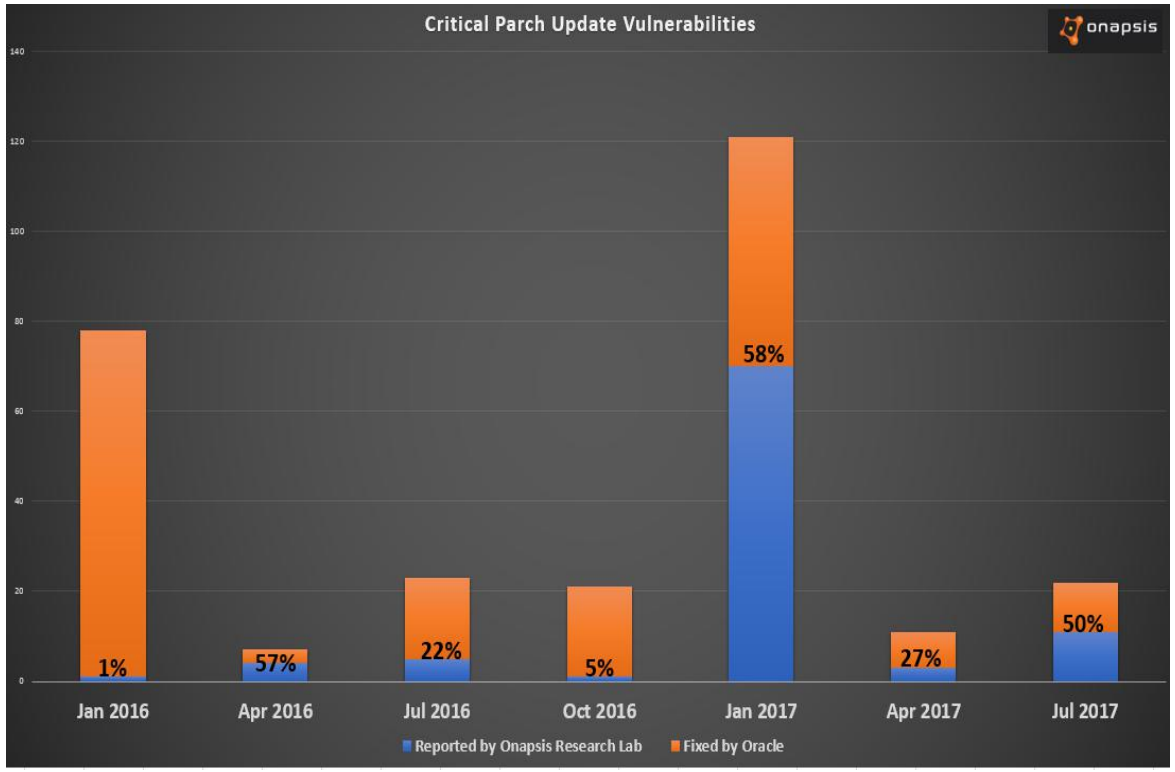
Traditional Security model is still applied to business-critical applications

- Auditors rely mostly on:
  - Segregation of Duties
  - Roles / Role to User Assignment / Approval Process
  - Emergency Access
  - Default accounts
  - Change Management Process
  - Governance, Risk and Compliance (GRC) tools
- All of the above items are necessary, but only address some insider threats. BUT what about Outsiders, Rogue Employees, Malware, State Sponsored Hacks?

Business-Critical Applications

Research contribution

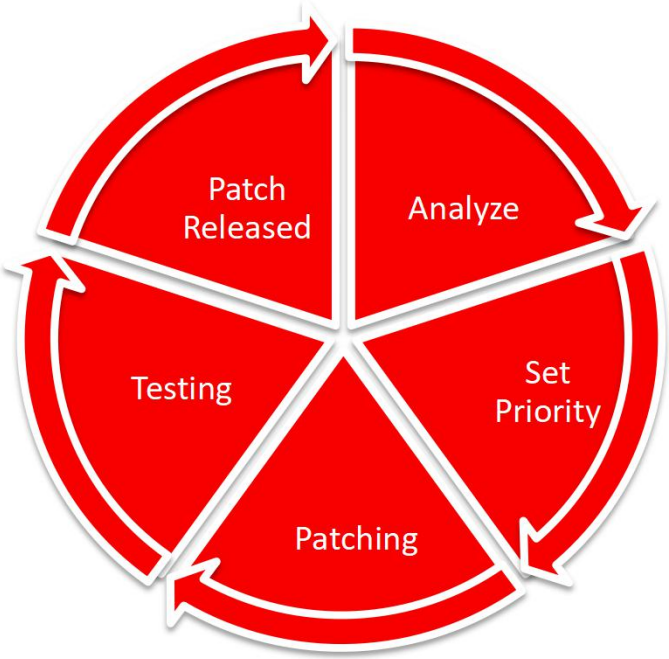
- The research community plays an important role in the security of these applications
- Over the last few years Onapsis collaborated with Oracle on helping secure Oracle E-Business Suite



Building the Patching Process

Five steps, recurrent process

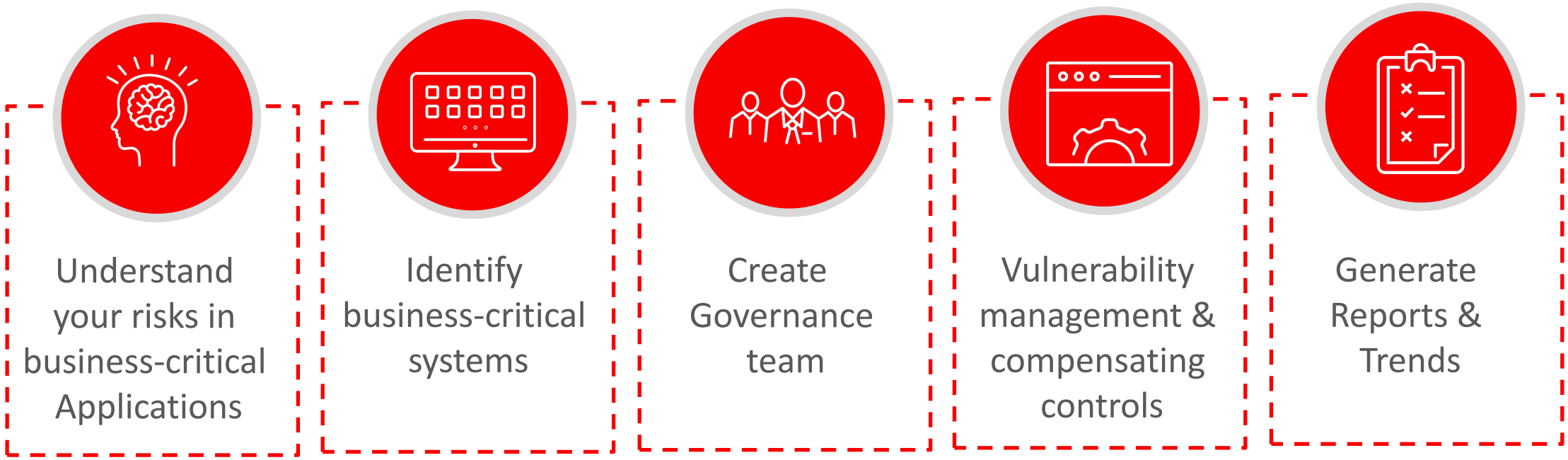
- Patches released
- Analysis
- Prioritization
- Patching
- Testing



Keeping up with Oracle's periodic release of CPU

- Defining what patches are applicable to your organization
- Defining which versions are vulnerable to the released patches
- Prioritizing patches based on Security or Compliance Mandates
- Defining system downtime while applying patches
- Checking for confirmation of proper implementation of patches
- Aligning patch management with internal security patch SLAs

Building the Governance Program



Creating an internal program helps bridge departments within the company and align them to the common goal of Oracle Cybersecurity while also achieving compliance

Bridging the teams

- Define the internal teams in your organization that should be involved
- Determine what Oracle security means to your organization
  - How mature do you want your security process to be
- Bridge communication between internal teams to form a common goal
- Begin Governance Program based on the security goals of the company, defined for business-critical applications
- Set reoccurring check-ins to confirm Program is on track and meeting the demands of each internal team

Involved Departments:

Information Security & CISOs

Internal Audit Teams

Apps DBA Teams
Oracle Security Teams

CIOs and
LOB owners

Risk Analysis for Your Organization

- Analysis of Critical Patch Update and Security Alerts risk matrices
  - Is the Oracle product attackable in my installation?
  - Are the installed version and components vulnerable?
  - What is the impact of a successful exploit?
  - How many potential attackers are there?
  - How difficult is the attack?
  - Is this vulnerability directly attackable or is the fix “security-in-depth” only?
- Key point: You must review the Risk Matrix factors

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSION 3.0 RISK (see Risk Matrix Definitions)									Supported Versions Affected	Notes
					Base Score	Attack Vector	Attack Complex	Privs Req'd	User Interact	Scope	Confid-entiality	Inte-grity	Avail-ability		
CVE-2017-9805	Oracle Retail XBRi Loss Prevention	Internal Operations (Struts 2)	HTTP	Yes	9.8	Network	Low	None	None	Un-changed	High	High	High	10.0.1, 10.5.0, 10.6.0, 10.7.0, 10.8.0, 10.8.1	

Oracle Security Advisories and Urgency of Patch Application

- Is the Oracle product attackable in my installation?
  - If the product is not used, it may still be installed (e.g. by default) and be vulnerable
- Are the installed version and components vulnerable?
  - Are the vulnerable versions installed?
  - Are the vulnerable components installed?

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSION 3.0 RISK (see Risk Matrix Definitions)									Supported Versions Affected	Notes
					Base Score	Attack Vector	Attack Complex	Privs Req'd	User Interact	Scope	Confid-entiality	Inte-grity	Avail-ability		
CVE-2017-9805	**Oracle Retail XBRi Loss Prevention**	**Internal Operations (Struts 2)**	HTTP	Yes	9.8	Network	Low	None	None	Un-changed	High	High	High	**10.0.1, 10.5.0, 10.6.0, 10.7.0, 10.8.0, 10.8.1**	

Oracle Security Alerts

- If the Oracle product version and component are installed and vulnerable AND if this is an **Oracle Security Alert** – Install immediately
  - Oracle only issues about two Security Alerts per year for over 1,000 products
  - Oracle Security Alerts are only issued for very serious vulnerabilities
  - Typically Security Alerts are issued when successful ongoing attacks are occurring or Oracle believes such attacks will be initiated very shortly

Oracle Security Alert - CVE-2017-9805

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSION 3.0 RISK (see Risk Matrix Definitions)									Supported Versions Affected	Notes
					Base Score	Attack Vector	Attack Complex	Privs Req'd	User Interact	Scope	Confid-entiality	Inte-grity	Avail-ability		
CVE-2017-9805	**Oracle Retail XBRi Loss Prevention**	**Internal Operations (Struts 2)**	HTTP	Yes	9.8	Network	Low	None	None	Un-changed	High	High	High	**10.0.1, 10.5.0, 10.6.0, 10.7.0, 10.8.0, 10.8.1**	

Impact of Successful Exploits

- What is the impact of a successful exploit?
  - Confidentiality: Unauthorized reading of data
  - Integrity: Unauthorized modification, deletion or creation of data
  - Availability: Unauthorized denial of access
  - Values:
    - 'None', 'Low' (partial compromise), 'High' (full compromise or partial with direct, serious threat)
  - All three 'High': Application takeover, Remote Code Execution
  - Scope: Containing component compromised (e.g. App Server or Op System)

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSION 3.0 RISK (see Risk Matrix Definitions)									Supported Versions Affected	Notes
					Base Score	Attack Vector	Attack Complex	Privs Req'd	User Interact	Scope	Confid-entiality	Inte-grity	Avail-ability		
CVE-2017-9805	Oracle Retail XBRi Loss Prevention	Internal Operations (Struts 2)	HTTP	Yes	9.8	Network	Low	None	None	**Un-changed**	**High**	**High**	**High**	10.0.1, 10.5.0, 10.6.0, 10.7.0, 10.8.0, 10.8.1	

Attack Vector

- Attack Vector
  - Values: ‘Network’, ‘Adjacent Network’ (same LAN Segment), ‘Physical’
  - Value ‘Local’:
    - Need logon to containing infrastructure (e.g. OS Logon)
    - Usually this means possible exploiters are limited to very few
    - If local logons are restricted to trusted people, Oracle fix would be considered “security in depth”

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSION 3.0 RISK (see Risk Matrix Definitions)									Supported Versions Affected	Notes
					Base Score	Attack Vector	Attack Complex	Privs Req'd	User Interact	Scope	Confid-entiality	Inte-grity	Avail-ability		
CVE-2017-9805	Oracle Retail XBRi Loss Prevention	Internal Operations (Struts 2)	HTTP	Yes	9.8	**Network**	Low	None	None	Un-changed	High	High	High	10.0.1, 10.5.0, 10.6.0, 10.7.0, 10.8.0, 10.8.1	

Privileges Required

- Privs Required
  - Values: ‘None’, ‘Low’, ‘High’
  - ‘Low’ versus ‘High’: Do privileges allow one to directly affect others? Yes=High
    - If High and only trusted have High, Oracle fix might be considered “security in depth”
    - Need logon to containing infrastructure (e.g. OS Logon)
    - Usually this means possible exploiters are limited to very few
  - If None and Network anyone with IP access can exploit

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSION 3.0 RISK (see Risk Matrix Definitions)									Supported Versions Affected	Notes
					Base Score	Attack Vector	Attack Complex	Privs Req'd	User Interact	Scope	Confid-entiality	Inte-grity	Avail-ability		
CVE-2017-9805	Oracle Retail XBRi Loss Prevention	Internal Operations (Struts 2)	HTTP	Yes	9.8	Network	Low	None	None	Un-changed	High	High	High	10.0.1, 10.5.0, 10.6.0, 10.7.0, 10.8.0, 10.8.1	

Attack Complexity, User Interaction

- Attack Complexity
  - Values: Assumes you have the attack already. If no special timing or other factors outside the control of the attacker then ‘Low’ else ‘High’
- User Interaction
  - Values: If a successful attack can occur without human interaction such as clicking on a link then ‘None’ else ‘Required’
- These factors indicate the “degree of difficulty” of a successful attack once an attack has been developed

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSION 3.0 RISK (see Risk Matrix Definitions)									Supported Versions Affected	Notes
					Base Score	Attack Vector	Attack Complex	Privs Req'd	User Interact	Scope	Confid-entiality	Inte-grity	Avail-ability		
CVE-2017-9805	Oracle Retail XBRi Loss Prevention	Internal Operations (Struts 2)	HTTP	Yes	9.8	Network	**Low**	None	**None**	Un-changed	High	High	High	10.0.1, 10.5.0, 10.6.0, 10.7.0, 10.8.0, 10.8.1	

CVSS Base Score

- CVSS base score is important but remember it is **base** score
  - CVSS >= 9.0 is generally critical but CVSS >= 2.0 can be used in a blended attack
  - Effective score often becomes “in-depth” if Authenticated or Local
  - Effective score often significantly reduced by firewalls/routers
  - Unauthenticated network attacks need particular attention

CVE#	Product	Component	Protocol	Remote Exploit without Auth.?	CVSS VERSION 3.0 RISK (see Risk Matrix Definitions)									Supported Versions Affected	Notes
					Base Score	Attack Vector	Attack Complex	Privs Req'd	User Interact	Scope	Confid-entiality	Inte-grity	Avail-ability		
CVE-2017-9805	Oracle Retail XBRi Loss Prevention	Internal Operations (Struts 2)	HTTP	Yes	9.8	Network	Low	None	None	Un-changed	High	High	High	10.0.1, 10.5.0, 10.6.0, 10.7.0, 10.8.0, 10.8.1	

Risk Analysis for Your Organization

- Analysis of Critical Patch Update and Security Alerts risk matrices
  - Is the Oracle product attackable in my installation?
  - Are the installed version and components vulnerable?
  - What is the impact of a successful exploit?
  - How many potential attackers are there?
  - How difficult is the attack?
  - Is this vulnerability directly attackable or is the fix “security-in-depth” only?
- Key point: Review the Risk Matrix factors

CVE#	Component	Package and/or Privilege Required	Protocol	Remote Exploit without Auth.?	CVSS VERSION 3.0 RISK (see Risk Matrix Definitions)									Supported Versions Affected	Notes
					Base Score	Attack Vector	Attack Complex	Privs Req'd	User Interact	Scope	Confid-entiality	Inte-grity	Avail-ability		
CVE-2017-3486	SQL*Plus	Local Logon	Oracle Net	No	7.2	Local	High	High	Required	Changed	High	High	High	11.2.0.4, 12.1.0.2	See Note 1
CVE-2017-3567	OJVM	Create Session, Create Procedure	Multiple	No	5.3	Network	High	Low	None	Un-changed	None	None	High	11.2.0.4, 12.1.0.2	

Conclusions

- Business-critical applications need to be properly deployed, monitored, and maintained
- Patching Oracle applications can pose some challenges, but the potential risk of not doing it is just too high!
  - Put a process in place to ensure it is consistently performed according to the pre-defined objectives
- Leverage Oracle's toolset, documentation and recommendations to streamline the process

Questions?

Integrated Cloud

Applications & Platform Services


ORACLE®