Security in knowledge

Why Does Database Patching Require A PhD?

Amichai Shulman, CTO

Michael Cherny, Data Security Research TL

IMPERVA

RSA CONFERENCE
EUROPE 2013

Session ID: ADS-W10
Session Classification: Advanced

Presenters

- CTO
- 25 years in Software Industry
- 20 years in Information Security

- Leading Data Security Research
- 17 years in Software Industry
- 13 years in Information Security

Agenda

- Vulnerability publishing and disclosure
- Oracle patching process review
- Oracle patch review process
- Finding the light
- My evil twin
- Risk management
- What we suggest

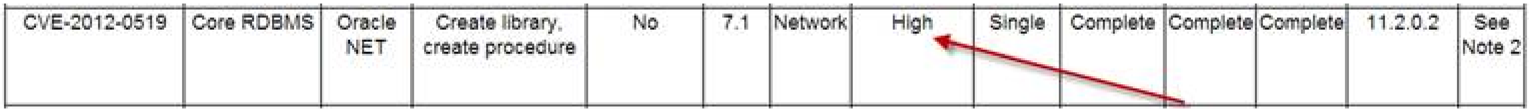
Vulnerability publishing and disclosure

- Usually discovered by third party
- Usually made public by vendor
  - In some cases years after vulnerability discovery
- Security by obscurity is a vendor’s choice
- Patch or nothing approach
- Real details almost never disclosed by vendor
- Customers are left to guesswork

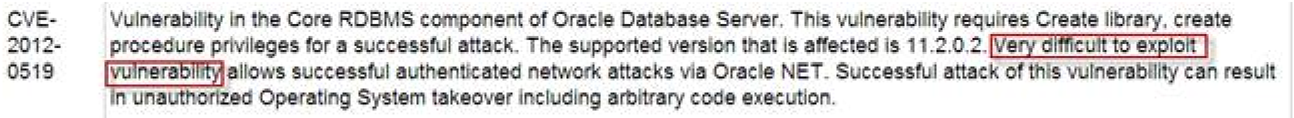
Oracle patching process review

- Every 3 month security patch is released
- Technical procedure being improved over the years
- Risk matrix documentation being improved over the years
- Real nature of vulnerabilities are not disclosed
- Workaround are suggested only if forced by 'irresponsible' disclosure

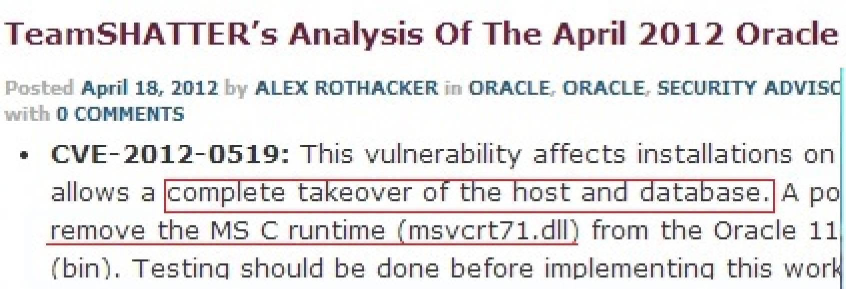
Example



CVE-2012-0519	Core RDBMS	Oracle NET	Create library, create procedure	No	7.1	Network	High	Single	Complete	Complete	Complete	11.2.0.2	See Note 2



CVE-2012-0519 Vulnerability in the Core RDBMS component of Oracle Database Server. This vulnerability requires Create library, create procedure privileges for a successful attack. The supported version that is affected is 11.2.0.2. Very difficult to exploit vulnerability allows successful authenticated network attacks via Oracle NET. Successful attack of this vulnerability can result in unauthorized Operating System takeover including arbitrary code execution.

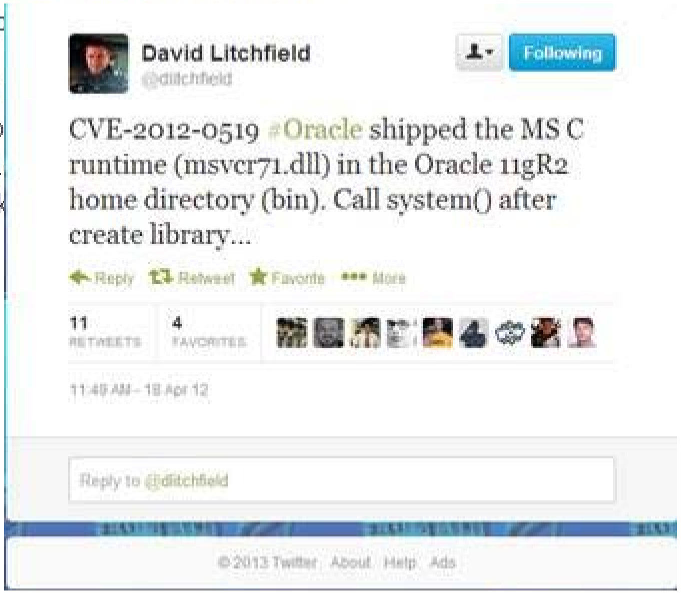


TeamSHATTER's Analysis Of The April 2012 Oracle CPU

TeamSHATTER Exclusive

Posted April 18, 2012 by ALEX ROTHACKER in ORACLE, ORACLE, SECURITY ADVISC
with 0 COMMENTS

- **CVE-2012-0519:** This vulnerability affects installations on
allows a complete takeover of the host and database. A po
remove the MS C runtime (msvcrt71.dll) from the Oracle 11
(bin). Testing should be done before implementing this work



David Litchfield
@dlitchfield

CVE-2012-0519 #Oracle shipped the MS C runtime (msvcr71.dll) in the Oracle 11gR2 home directory (bin). Call system() after create library...

Oracle patch review process

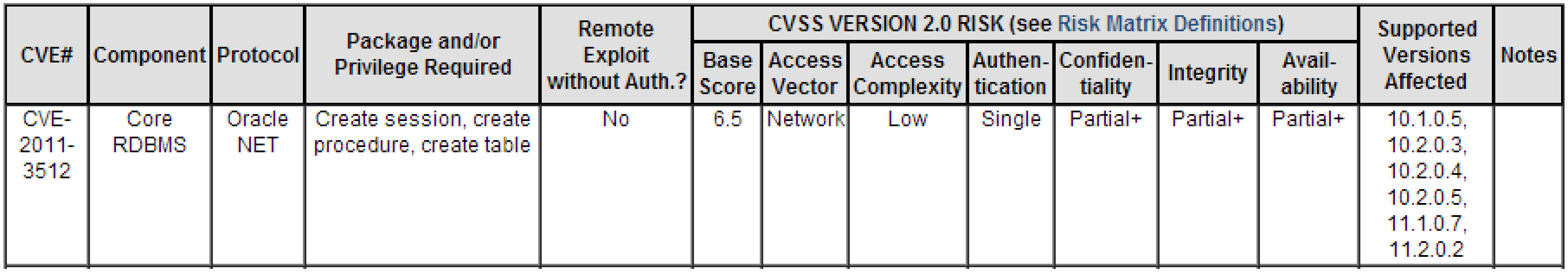
- Security vendors are following Oracle CPUs
- Vulnerability assessment
- Virtual patching
- Security vendors are left in the dark
- Security product updates are slowed
- Customers with longer patching cycle are left without alternative

Oracle patch review process (cont.)

- Review what Oracle published
- Read between the lines of risk matrix
- For every CVE search for clues published by third party researchers
- Unpack new packages and compare to previous version
- Reverse engineer vulnerability

Finding the light

- CVE-2011-3512



CVE#	Component	Protocol	Package and/or Privilege Required	Remote Exploit without Auth.?	CVSS VERSION 2.0 RISK (see Risk Matrix Definitions)							Supported Versions Affected	Notes
					Base Score	Access Vector	Access Complexity	Authentication	Confidentiality	Integrity	Availability		
CVE-2011-3512	Core RDBMS	Oracle NET	Create session, create procedure, create table	No	6.5	Network	Low	Single	Partial+	Partial+	Partial+	10.1.0.5, 10.2.0.3, 10.2.0.4, 10.2.0.5, 11.1.0.7, 11.2.0.2	

- TeamSHATTER:
  - SQL Injection Vulnerability in Oracle DROP INDEX for spatial datatypes.
  - Oracle Database supports spatial datatypes. A vulnerability exists in the handling of spatial indexes. Users with create table and create procedure privileges can elevate their privileges to SYSDBA (CVE-2011-3512).
  - Fix: Apply Oracle Critical Patch Update October 2011 available at Oracle Support.

Demo – from darkness to light

My evil twin

- Being my twin, same knowledge is gathered
- Being evil…

Demo - tool

Security in knowledge

Risk management

- DB owners cannot complete a reasonable risk assessment process
- Non-informed security decisions are made with respect to their mission critical systems

What we suggest

- Knowing the true nature of vulnerability:
  - Enables true risk assessment by DB owners
  - Workarounds can be implemented
    - Uninstall vulnerable package
    - Implementing controls (monitor index creating with susceptible names)
  - Security professionals can provide the immediate necessary assistance

- Vendors should implement responsible information sharing procedures

Thank you!

Amichai Shulman, CTO

shulman@imperva.com

Michael Cherny, Data Security Research TL

cherny@imperva.com

RSA CONFERENCE
EUROPE 2013

#RSAC

Security in knowledge

RSA CONFERENCE
EUROPE 2013

Session ID:

Session Classification:

Security in knowledge

RSA CONFERENCE EUROPE 2013

#RSAC

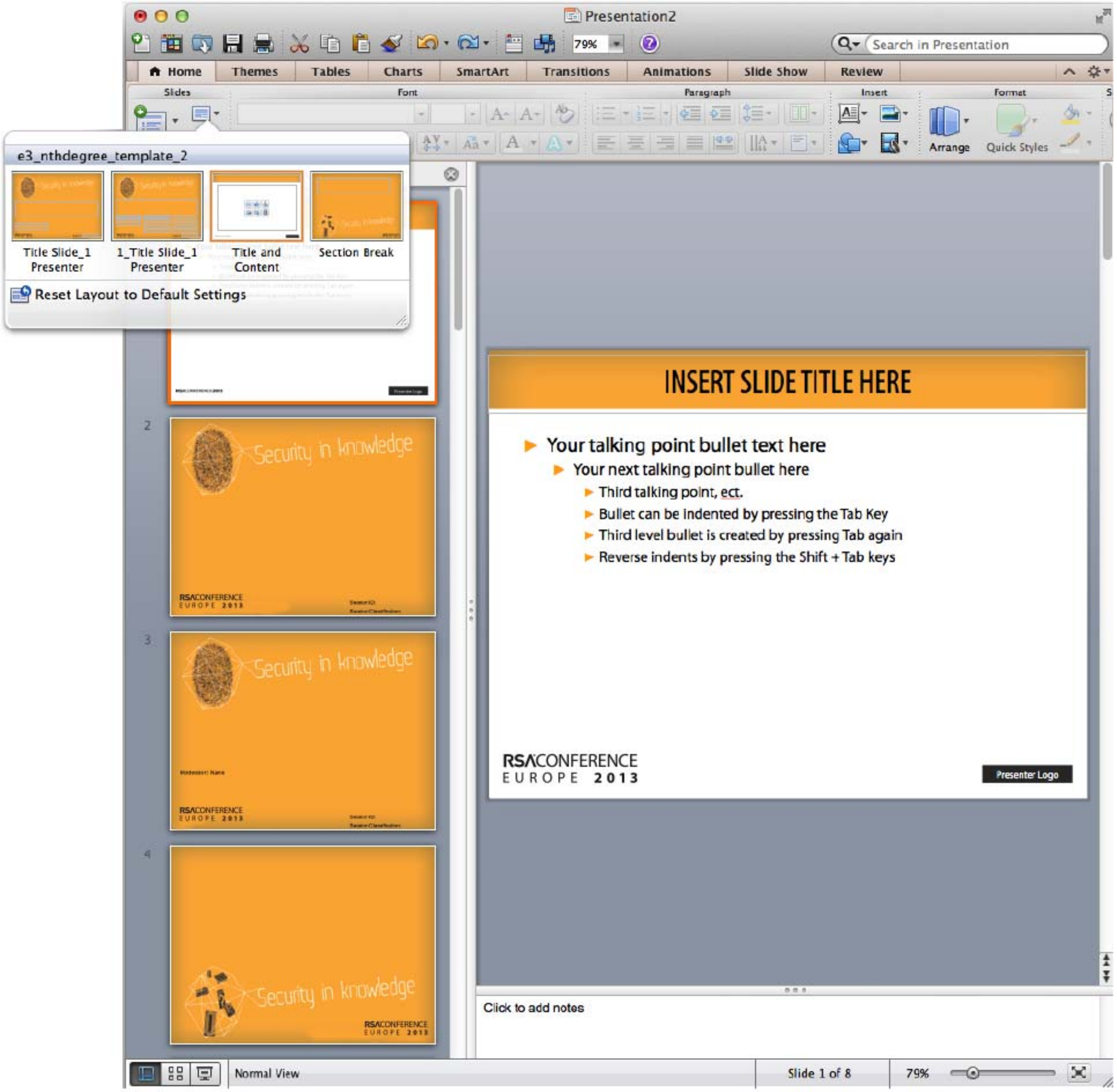
Thank you!

PLEASE READ

- Background art, fonts, and the color palette have been formatted for you in the Slide Master.
- The fonts for this presentation are **Myriad Pro Cond** (titles) and **Myriad Pro** (body text) . Please use only these fonts, or their Mac equivalents.
- Line-spacing for bullets has been set for you. There should **not** be a need to add an extra “carriage return” (Enter key) between bullets.
- Read the “Helpful Hints” provided in the notes page (in the “View” menu) of this slide.

USING THIS TEMPLATE

There are 4 pre-formatted slide layouts for you to use. These can be accessed in the **LAYOUT** window of the **HOME** ribbon



INSERT SLIDE TITLE HERE

- Your talking point bullet text here
  - Your next talking point bullet here
    - Third talking point, ect.
    - Bullet can be indented by pressing the Tab Key
    - Third level bullet is created by pressing Tab again
    - Reverse indents by pressing the Shift + Tab keys

RSACONFERENCE EUROPE 2013

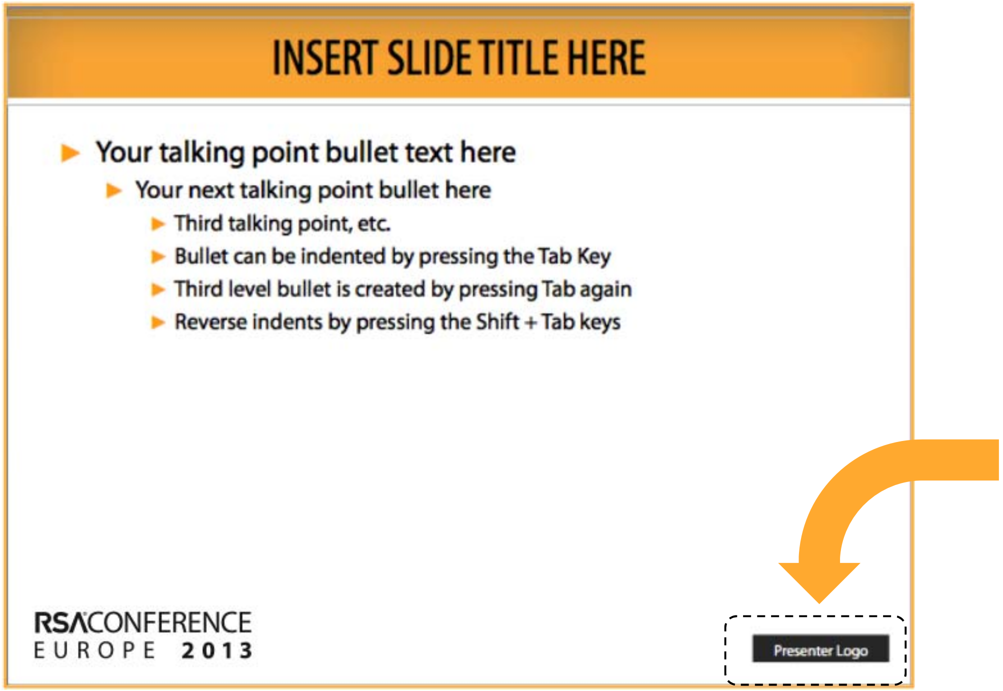
Click to add notes

USING THIS TEMPLATE

This template has been designed to allow you to insert your own logo in the lower right corner of the content slide.

To insert:

1. View > Slide Master
2. In the left-hand window, scroll to the top and click on the uppermost template. (Important! Do not skip this step!)
3. Click on the placeholder box at lower right and delete
4. Insert > Picture and browse to your logo art
5. Resize logo art as needed
6. View>Normal



INSERT SLIDE TITLE HERE

- Your talking point bullet text here
  - Your next talking point bullet here
    - Third talking point, etc.
    - Bullet can be indented by pressing the Tab Key
    - Third level bullet is created by pressing Tab again
    - Reverse indents by pressing the Shift + Tab keys

RSACONFERENCE EUROPE 2013

Presenter Logo