



# CPU-Info

3/2011

Komentarze i testy  
do Oracle Critical Patch Update  
lipiec 2011



OPITZ CONSULTING



## Spis treści

---

<b>1</b>	<b>Wprowadzenie.....</b>	<b>3</b>
<b>2</b>	<b>Podstawy .....</b>	<b>4</b>
2.1	Analiza Oracle Technology Network (OTN) i Oracle Metalink.....	4
2.2	Analiza dodatkowych źródeł .....	4
<b>3</b>	<b>Ocena ogólna CPU .....</b>	<b>5</b>
<b>4</b>	<b>Wprowadzone poprawki zabezpieczeń dla Oracle Database Server .....</b>	<b>7</b>
<b>5</b>	<b>Wyniki testów instalacji CPU na różnych systemach.....</b>	<b>12</b>
5.1	Opis instalacji CPU .....	12
5.2	Wyniki przeprowadzonych testów .....	13
<b>6</b>	<b>Glosariusz.....</b>	<b>15</b>
<b>7</b>	<b>Uwagi prawne .....</b>	<b>15</b>

## 1 Wprowadzenie

---

### Witamy Państwa serdecznie na stronach naszego aktualnego CPU-Info

Z myślą o naszych klientach krótko po opublikowaniu Oracle *Critical Patch Update* (CPU) 19-go lipca 2011 wspólnie z firmą Red DataBase Security sporządziliśmy zestawienie usuniętych błędów oraz dokonaliśmy szczegółowej analizy łącznie 78 poprawek znajdujących się w poniższym CPU.

Tę usługę oferujemy Państwu bezpłatnie w formie dokumentu PDF. Zawiera ona ponadto testy instalacji CPU przeprowadzone na różnych platformach i wersjach bazy danych Oracle.

Chcielibyśmy Państwa wesprzeć w instalacji zestawu poprawek CPU, nadając jej bardziej przystępną i przyswajalną formę.

Pytania i komentarze prosimy kierować na adres:



**Piotr Sajda**  
*Kierownik Działu Service Engineering (SE)*

OPITZ CONSULTING Kraków Sp. z o.o.  
Bratysławska 1A  
31-201 Kraków  
tel. +48 12 617 1810  
kom. +48 519 309 710  
[Piotr.Sajda@opitz-consulting.com](mailto:Piotr.Sajda@opitz-consulting.com)  
[www.opitz-consulting.pl](http://www.opitz-consulting.pl)



**Grzegorz Jakusz-Gostomski**  
*Starszy Konsultant*

OPITZ CONSULTING Kraków Sp. z o.o.  
Bratysławska 1A  
31-201 Kraków  
tel. +48 12 617 1807  
kom. +48 519 309 707  
[Grzegorz.Jakusz-Gostomski@opitz-consulting.com](mailto:Grzegorz.Jakusz-Gostomski@opitz-consulting.com)  
[www.opitz-consulting.pl](http://www.opitz-consulting.pl)

## 2 Podstawy

---

### 2.1 Analiza Oracle Technology Network (OTN) i Oracle Metalink

Podstawą przeprowadzonej analizy są niżej wymienione źródła jak i własne badania:

Przegląd Patch Set Updates i Critical Patch Updates:

<http://www.oracle.com/technetwork/topics/security/alerts-086861.html>

Ogólne informacje dotyczące Oracle CPU, kwiecień 2011:

<http://www.oracle.com/technetwork/topics/security/cpuapr2011-301950.html>

Macierz ryzyka dla RDBMS w Oracle CPU, kwiecień 2011:

<http://www.oracle.com/technetwork/topics/security/cpuapr2011-301950.html#AppendixDB>

Oracle Patch Set Update i Critical Patch Update kwiecień 2011 – dostępność [ID 1291877.1]:

<https://support.oracle.com/CSP/main/article?cmd=show&type=NOT&id=1291877.1>

Map of Public Vulnerability to Advisory/Alert:

<http://www.oracle.com/technetwork/topics/security/public-vuln-to-advisory-mapping-093627.html>

Oracle Critical Patch Update, kwiecień 2011 – Database Patch Security Vulnerability Molecule Mapping [ID 1291868.1]:

<https://support.oracle.com/CSP/main/article?cmd=show&type=NOT&id=1291868.1>

Oracle Critical Patch Update, kwiecień 2011 – Database Known Issues [ID 1291830.1]:

<https://support.oracle.com/CSP/main/article?cmd=show&type=NOT&id=1291830.1>

Oracle Critical Patch Update, kwiecień 2011 – Documentation Map [ID 1305064.1]:

<https://support.oracle.com/CSP/main/article?cmd=show&type=NOT&id=1305064.1>

Oracle Critical Patch Update, kwiecień 2011 – pliki Readme:

Oracle 10.1.0.5, 10.2.0.4, 10.2.0.5, 11.1.0.7, 11.2.0.1, 11.2.0.2

Critical Patch Update July 2011 Oracle Enterprise Manager Grid Control Known Issues [ID 1323600.1]:

<https://support.oracle.com/CSP/main/article?cmd=show&type=NOT&id=1323600.1>

### 2.2 Analiza dodatkowych źródeł

Przy opracowaniu zastosowane zostały zewnętrzne źródła:

<http://www.red-database-security.com>

<http://cve.mitre.org>

<http://nvd.nist.gov/cvss.cfm?calculator&adv&version=2>

<http://www.firmenpresse.de/pressrelease31277.html>

<http://www.computerweekly.com/Articles/2011/07/20/247345/Oracle-should-take-a-closer-look-at-security-and-severity-scoring-says.htm>

### 3 Ocena ogólna CPU

---

W CPU z lipca 2011 znaleźć można łącznie 78 poprawki do produktów Oracle, a tym samym trochę więcej niż w poprzedniej edycji (styczeń 2011: 66, kwiecień 2011: 73). Poprawki podzielone są na następujące grupy produktów:

- Oracle Database
- Oracle Fusion Middleware
- Oracle Enterprise Manager
- Oracle Applications – E-Business Suite
- Oracle Applications – Oracle PeopleSoft Enterprise, JD Edwards, Siebel i Oracle Supply Chain Product Suite
- Oracle Health Sciences Applications
- Oracle Sun Products Suite

Większość poprawek w odniesieniu do liczby usuniętych błędów odnosi się znów do Sun Products Suite. Przypadają na nie 23 rozwiązania. W tej grupie usunięto najwyżej oceniany błąd, bo aż 10,0 Base Score. Dotyka on produktów SPARC T3-1, SPARC T3-1B, SPARC T3-2, SPARC T3-4, Netra SPARC T3-1, Netra SPARC T3-1B.

W aktualnym CPU warto zauważyć, że wieloma poprawkami objęto komponenty Enterprise Manager Grid Control – oddano do dyspozycji 17 rozwiązań dla tego produktu. Problemami tymi dotknięte są również bazy danych, które korzystają z Database Control.

W Oracle Database Server rozwiązaniami objęto 16 luk w bezpieczeństwie. Jest to wyraźnie więcej niż w poprzednim CPU (styczeń 2010: 9, kwiecień 2010: 7, lipiec 2010: 6, październik 2010: 8, styczeń 2011: 5, kwiecień 2011: 6). Aktualne CPU rozwiązuje także 13 problemów z bezpieczeństwem dotyczących Database Server. Dwie z tych luk oprócz Oracle Database Server występują również w Oracle Client (CVE-2011-2231, CVE-2011-2232): Jeżeli zainstalowane są aplikacje klienckie, które używają XML Developer Kit, wówczas instalacja CPU jest konieczna, aby chronić należące do nich aplikacje. Atak poprzez klientów na Oracle Database Server nie jest możliwy, jeśli zainstalowano aktualne CPU. Trzy z 16 łącznie zaproponowanych rozwiązań dla Database Server dotyczą Secure Backup. Luki w bezpieczeństwie ocenione zostały w tym przypadku, podobnie jak i w poprzednich - bardzo wysoko (10,0, 6,8 i 4,3).

Aktualne CPU obejmuje pewne zmiany oraz trudności dotyczące OPatch-Tool. W wersji 10.1.0.5 występuje błąd dotyczący Universal Installer – a przez to też OPatch (patrz: CVE-2011-2240).

Universal Installer zabezpieczony jest przez aktualizację Database Server. Odnośnie OPatcha jest jeden minimalny wymóg: wersja 1.0.0.0.64. Również wersje 11.1 oraz 11.2 zostały zaktualizowane w ostatnich tygodniach. Jednakże pierwsza próba zainstalowania nowego OPatch dla PSU w Oracle Database Server Release 11.2.0.1 nie powiodła się (stan z 21.07.2011). Dla wersji 11.2.0.2 nie stwierdzono żadnych problemów.

Jeżeli zsumujemy wszystkie luki w Oracle Database Server (z Secure Backup włącznie) oraz te występujące w Enterprise Managers Grid Control, które również dotyczą komponentów bazy danych, otrzymamy 33 rozwiązania. Base Scores dla tych luk jest względnie wysoki. Najwyższą oceną dla bazy danych wynosi 7,1. Większość ocen w skali Base Scores dla Enterprise Manager Grid Control plasuje się pomiędzy 6 a 7. Najwyższa ocena w dziedzinie Secure Backup wynosi 10,0. Dlatego zdecydowanie zaleca się instalację aktualnego CPU dla produktów Oracle Database Server, Secure Backup jak również Enterprise Manager Grid Control.

Dla wersji 10.2.0.4 oraz 11.2.0.1 Database Server po aktualnym CPU nie będzie już żadnych nowych. Wyjątek stanowią platformy Oracle Solaris x86 (32-bit) i Apple Mac OS X, dla których kolejne wydania CPU będą wydawane – jako datę końcową podaje się dla nich lipiec 2013. Klienci korzystający z wersji 10.2.0.4 i 11.2.0.1, powinni w tym czasie zaktualizować swoje bazy danych do możliwie najwyższej dostępnej wersji.

Kolejne edycje Oracle CPU zaplanowano na 18-go października 2011 i 17 stycznia 2012. Styczniowy CPU 2012 będzie ostatnim Critical Patch Update dla bazy danych wersji 10.1.0.5.

## 4 Wprowadzone poprawki zabezpieczeń dla Oracle Database Server

---

Poniżej zamieszczony został opis i ocena luk w bezpieczeństwie, które zostały rozwiązane w lipcowym CPU 2011 w Database Server, Enterprise Manager Grid Control i Oracle Secure Backup:

### **CVE-2011-2239 Core RDBMS (10.2.0.3, 10.2.0.4, 10.2.0.5, 11.1.0.7, 11.2.0.1, 11.2.0.2)**

Luka została oceniona najwyżej w base score (7,1) dla Oracle Database Server. Jeżeli luka nie zostanie zabezpieczona, atak poprzez sieć może spowodować downtime, który może iść w parze z manipulacją danych. Atak możliwy jest pod warunkiem, że jest dostęp do pakietu XMLSEQ\_IMP\_T. Aby wykorzystać tę lukę w bezpieczeństwie, napastnik musi mieć dostępną odpowiednią wersję.

### **CVE-2011-2253 Core RDBMS (10.2.0.3, 10.2.0.4, 10.2.0.5, 11.1.0.7, 11.2.0.1, 11.2.0.2)**

Również w tym przypadku base score oszacowano na 7,1. Przypuszczalnie atakujący, który posiada uprawnienia SYSDBA, może sobie również zabezpieczyć odwrót, który umożliwi mu dostęp jako SYSDBA nawet po odebraniu tych uprawnień poprzez „revoke sysdba from“. Atak tą drogą może zaowocować nieplanowanymi przerwami w dostępie usług i manipulacją danych. Ponieważ do wykorzystania tej luki potrzebne są minimum uprawnienia „initial SYSDBA“, ryzyko zostało ocenione nieco niżej niż sugerowany base score 7,1.

**CVE-2011-0882 (Oracle Enterprise Manager Grid Control) Content Management (10.1.0.5, 10.2.0.3, 10.2.0.4, 11.1.0.7) / CVE-2011-2257 (Oracle Enterprise Manager Grid Control) Database Target Type Menus (10.1.0.5, 10.2.0.3, 10.2.0.4, 10.2.0.5, 11.1.0.7, 11.2.0.1, 11.2.0.2) / CVE-2011-2248 (Oracle Enterprise Manager Grid Control) SQL Performance Advisories/UIs (11.1.0.7, 11.2.0.1, 11.2.0.2) / CVE-2011-0870 (Oracle Enterprise Manager Grid Control) Schema Management (10.1.0.5, 10.2.0.3, 10.2.0.4, 10.2.0.5, 11.1.0.7, 11.2.0.1, 11.2.0.2) / CVE-2011-0848 (Oracle Enterprise Manager Grid Control) Security Framework (10.1.0.5, 10.2.0.3, 10.2.0.4, 10.2.0.5, 11.1.0.7, 11.2.0.1, 11.2.0.2) / CVE-2011-0852 (Oracle Enterprise Manager Grid Control) Security Management (10.1.0.5, 10.2.0.3, 10.2.0.4) / CVE-2011-0822 (Oracle Enterprise Manager Grid Control) Streams, AQ & Replication Mgmt (10.1.0.5, 10.2.0.3)**

Powyzsze luki oceniono łącznie. Co prawda dotyczą różnych komponentów, ale sposób przeprowadzenia ataku, konieczna wiedza do niego oraz ocena ryzyka są podobne. Dotknięte są Enterprise Manager Grid Control oraz odpowiadające im komponenty Database Control, a także pośrednio zarządzane w ten sposób bazy danych. Sposób przeprowadzenia ataku (http, remote i bez autentykacji) w odpowiedniej kombinacji ocenione w base score na 6,8 każą przypuszczać,

że ataki następują poprzez Cross-Site-Scripting. Może to prowadzić do manipulowania danymi i przerw w dostawie usług.

**CVE-2011-0835 Core RDBMS (11.1.0.7, 11.2.0.1, 11.2.0.2)**

Niestety niewiele wiadomo o tej luce. Base score jest stosunkowo wysoki i wynosi 6,5. W prosty sposób posiadając uprawnienie „create session” można zmienić dane, co może powodować również nieplanowane przerwy.

**CVE-2011-0880 Core RDBMS (11.1.0.7, 11.2.0.1, 11.2.0.2)**

Podobnie jak **CVE-2011-0835** nie znamy szczegółów dot. CVE-2011-0880. Base Score wynosi również 6,5 i wystarcza uprawnienie „create session”, aby dokonać ataku na bazę danych.

**CVE-2011-0838 Core RDBMS (11.1.0.7, 11.2.0.1, 11.2.0.2)**

To trzecia luka w bezpieczeństwie, która pasuje się podobnie jak obydwie opisane powyżej **CVE-2011-0835** i **CVE-2011-0880**. W tym przypadku obok „create session”- potrzebne są jeszcze uprawnienia „create procedure”, aby dokonać odczytu danych, ich zmiany albo ograniczenia dostępności serwera.

**CVE-2011-2244 (Oracle Enterprise Manager Grid Control) Security Framework (10.1.0.5, 10.2.0.3, 10.2.0.4, 10.2.0.5, 11.1.0.7, 11.2.0.1, 11.2.0.2)**

Luka dotyczy Enterprise Manager Grid Control i pozwala na odczyt i zmianę danych poprzez sieć. Nie ogranicza jednak dostępności, stąd ocenia base score wynosi 6,4.

**CVE-2011-0832 Core RDBMS (11.1.0.7, 11.2.0.1, 11.2.0.2)**

Base score dla tej luki wynosi 6,0. Następstwami ataku mogą być manipulowanie danymi oraz nieplanowane przerwy w dostawie usług. Aby wykorzystać lukę wystarcza uprawnienie „create session. Również odnośnie tego problemu nie ma w tym momencie bardziej szczegółowych informacji.

**CVE-2011-2232 XML Developer Kit (10.1.0.5, 10.2.0.3, 10.2.0.4, 11.1.0.7, 11.2.0.1)**

XML Developer Kit zawiera lukę bezpieczeństwa ocenioną w base score na 6,0. Dla ochrony serwera bazy danych powinno się zainstalować proponowanego patcha. Dodatkowo, aby uchronić aplikację zaleca się pilną instalację aktualizacji klientów wykorzystujących XML Developer Kit.

**CVE-2011-0816 (Oracle Enterprise Manager Grid Control) CMDB Metadata & Instance APIs (10.1.0.5, 10.2.0.3, 10.2.0.4, 10.2.0.5, 11.1.0.7, 11.2.0.1, 11.2.0.2) / CVE-2011-0875 (Oracle Enterprise Manager Grid Control) EMCTL (11.1.0.7) / CVE-2011-0831 (Oracle Enterprise Manager Grid Control) Enterprise Config Management (10.1.0.5, 10.2.0.3, 10.2.0.4, 10.2.0.5, 11.1.0.7, 11.2.0.1, 11.2.0.2)**

Te komponenty dotyczą luki w bezpieczeństwie oszacowane wg base score na 5,5. Manipulacja danymi można nastąpić przez sieć i nie wymaga żadnych szczególnych uprawnień.

**CVE-2011-2230 Core RDBMS (10.1.0.5, 10.2.0.3, 10.2.0.4, 10.2.0.5, 11.1.0.7, 11.2.0.1)**

Odnosnie luki CVE-2011-2230 w danym momencie nie ma dostępnych szczegółów. Base score w odniesieniu do matrycy ryzyka wynosi 5,0. Odczyt danych lub ich zmiana przez atakującego nie są możliwe, jednakże dostępność może być ograniczona.

**CVE-2011-0811 (Oracle Enterprise Manager Grid Control) Enterprise Config Management (10.1.0.5, 10.2.0.3, 10.2.0.4)**

Atak może nastąpić lokalnie przez Enterprise Manager Grid Control. Base score wynosi 4,9.

**CVE-2011-0881 (Oracle Enterprise Manager Grid Control) EMCTL (10.2.0.3, 10.2.0.4, 11.1.0.7) / CVE-2011-0876 (Oracle Enterprise Manager Grid Control) Enterprise Manager Console (10.1.0.5, 10.2.0.3, 10.2.0.4, 10.2.0.5, 11.1.0.7, 11.2.0.1, 11.2.0.2) / CVE-2011-0830 (Oracle Enterprise Manager Grid Control) Event Management (10.1.0.5, 10.2.0.3, 10.2.0.4) / CVE-2011-0877 (Oracle Enterprise Manager Grid Control) Instance Management (10.1.0.5, 10.2.0.3, 10.2.0.4) / CVE-2011-0879 (Oracle Enterprise Manager Grid Control) Instance Management (10.1.0.5, 10.2.0.3, 10.2.0.4, 10.2.0.5, 11.1.0.7, 11.2.0.1, 11.2.0.2)**

Ocena tych pięciu luk jest wspólna a base score wynosi 4,3. Jak zwykle w Grid Control – ataki mogą następować przez HTTP. Luki te mogą prowadzić do przerw w dostawie usług, manipulowanie danymi nie jest możliwe.

**CVE-2011-2231 XML Developer Kit (10.1.0.5, 10.2.0.3, 10.2.0.4, 10.2.0.5, 11.1.0.7, 11.2.0.1)**

Kolejna luka, podobnie jak CVE-2011-2232, dotyczy XML Developer Kit. Base score oszacowany został na 4,3, a więc niżej niż opisana luka. Również w tym przypadku powinno się, oprócz serwera bazy danych – dodatkowo zaktualizować klienta.

**CVE-2011-2238 Database Vault (10.2.0.3, 10.2.0.4, 10.2.0.5, 11.1.0.7, 11.2.0.1)**

Utrudnienie w tym przypadku polega na tym, że Database Vault można obejść. Za pomocą uprawnień „execute“ do DBMS\_SYS\_SQL można zamienić kontekst użytkownika na użytkownika docelowego i pod nim wykonać inne czynności. Jeżeli zapytanie w tabelach innego schematu sprawdza w Database Vault uprawnienia takie jak np. „select any table“ Database Vault, to po zamianie kontekstu kontrola uprawnień już nie występuje, a zapytanie jest wykonywane tak, jakby było wykonywane na „własnej“ tabeli. Base score dla tej luki w bezpieczeństwie został oszacowany na 4,0. Danymi można częściowo manipulować.

#### **CVE-2011-2243 Core RDBMS (11.1.0.7.3, 11.2.0.1, 11.2.0.2)**

Ta luka bezpieczeństwa – wskazana przez Alexandra Kornbrusta – utrudnia monitoring zdarzeń związanych z bezpieczeństwem. Wprawdzie można uruchomić triggery, przy których określone zdarzenia (np. wielokrotne błędne logowanie) będą monitorowane, a powiadomienie o tym przesyłane mailem. Ten mechanizm nie funkcjonuje poprawnie przy określonych zdarzeniach w wersjach 11.1.0.7.3, 11.2.0.1, jak również 11.2.0.2 i wówczas trigger po wystąpieniu tychże nie zostaje uruchomiony. Powiadomienia o atakach w określonych warunkach nie zostaną wygenerowane i wysłane, a przez to mogą pozostać niezauważone.

#### **CVE-2011-2240 Oracle Universal Installer (10.1.0.5)**

W lipcowym CPU 2011 opublikowany został patch dla Universal Installera. Base score wynosi tylko 1,7. Lukę można wykorzystać tylko podczas lokalnego dostępu. Kolejnym uwarunkowaniem jest dostęp do systemu plików.

#### **CVE-2011-2242 Core RDBMS (11.2.0.1, 11.2.0.2)**

W tym przypadku base score wynosi 1,3. Atak jest możliwy za pomocą protokołu FTP, przez lokalne konto jak również konto w bazie danych z prawem do logowania do XML DB FTP.

#### **CVE-2011-2261 Oracle Secure Backup (10.3.0.3)**

Tą lukę bezpieczeństwa w systemach Windows oceniono na 10,0 w Linux na 7,5, na platformach Unix i innych ryzyko zostało ocenione maksymalnie. Zaleca się pilnie instalację najnowszej wersji Secure Backup. Bez autoryzacji czy wykorzystania specjalnych uprawnień atakujący może przez sieć przejąć pełną kontrolę nad serwerem.

#### **CVE-2011-2252 Oracle Secure Backup (10.3.0.3)**

Również tę lukę, ocenioną na 6,8 wg wskaźnika ryzyka base score, można wykorzystać bez szczególnych uprawnień z wykorzystaniem zdalnego dostępu, a w ten sposób spowodować

przerwy w dostawie usług lub utratę danych. Oracle stosuje w tym przypadku ocenę „Partial+“ dla skutków ewentualnego ataku. „Partial+“ jest wprawdzie dodatkiem Oracle do oficjalnej skali CVSS, która szacowana jest tylko jak „Partial“, chociaż ryzyko jest większe. Dlatego też wskazane jest branie pod uwagę zagrożenia większego niż ocenione w base score na 6,8.

### **CVE-2011-2251 Oracle Secure Backup (10.3.0.3)**

Luka CVE-2011-2251 jest podobna i równie łatwa do wykorzystania jak wcześniej wymienione luki Oracle Secure Backup. Skutki wykorzystania luki nie są tak duże, co w efekcie dało ocenę 4,3 base Score.

### **Podsumowanie 11.2.0.2:**

Na Database Server w wersji 11.2.0.2 przypada osiem luk bezpieczeństwa, które można rozwiązać dzięki lipcowemu CPU 2011. Dodatkowo w tym przypadku występują luki, które dotyczą użytkowników Enterprise Manager Grid Control lub Database Control. Ponieważ wskaźnik ryzyka jest wysoki, zaleca się pilną instalację aktualnego CPU.

### **Podsumowanie 11.2.0.1:**

W tym przypadku zalecenie jest podobne jak dla wersji 11.2.0.2.: instalacja najnowszej wersji CPU. W ten sposób rozwiązanie znajdzie 12 luk w bezpieczeństwie dla Database Server w wersji 11.2.0.1. Do tego dochodzą rozwiązania luk dla Enterprise Manager Grid Control. Również dla Oracle Clients powinno się zainstalować aktualizację, jeżeli korzystają z XML Developer Kit.

### **Podsumowanie 11.1.0.7:**

Database Server Version 11.1.0.7. jest również dotknięta dziewięcioma lukami w bezpieczeństwie serwera bazy danych, które rozwiązuje aktualny CPU. Dlatego zalecamy jego instalację. Zalecenie to dotyczy również użytkowników Enterprise Manager Grid Control czy Database Control. Oracle Clients powinny również zostać zaktualizowane, o ile korzystają z XML Developer Kit.

### **Podsumowanie 10.2.0.5:**

Pięć luk bezpieczeństwa dla wersji 10.2.0.5 zostało rozwiązanych. Mimo, że w porównaniu z innymi wersjami to niewiele, instalacja aktualnego CPU jest wskazana, ponieważ wskaźniki ryzyka zostały ocenione w tych przypadkach dość wysoko. Również te błędy dotyczą użytkownika Enterprise Manager Grid Control oraz Oracle Clients.

### **Podsumowanie 10.2.0.4:**

Zalecenie dla Database Server w wersji 10.2.0.4 jest takie samo, jak w przypadku 10.2.0.5. CPU z lipca 2011 zamyka 6 luk w bezpieczeństwie i dlatego powinno się je koniecznie zainstalować. Również w tym przypadku w określonych warunkach dotknięte są Oracle Clients.

### Podsumowanie 10.2.0.3:

Najwyższa ocena wg base score dla Database Server w wersji 10.2.0.3 to 7,1. Również w tym przypadku zaleca się zastosowanie CPU z lipca 2011. Rozwiązuje ono 6 problemów z bezpieczeństwem dla tej wersji, dodatkowo także luki dotyczące Enterprise Manager Grid Control. Problemy z Oracle Clients muszą również zostać wzięte pod uwagę, jeżeli XML Developer Kit jest w użyciu.

### Podsumowanie 10.1.0.5:

Podobnie jak w innych przypadkach, instalacja aktualnego CPU jest również zalecana dla wersji 10.1.0.5. Także tutaj uwzględnienia wymagają Enterprise Manager Grid Control oraz ewentualnie Oracle Clients.

### Podsumowanie Oracle Secure Backup 10.3.0.3:

Aktualizacja Oracle Secure Backup jest pilnie zalecana, aby zminimalizować ewentualne ataki i ich ewentualne następstwa.

## 5 Wyniki testów instalacji CPU na różnych systemach

### 5.1 Opis instalacji CPU

Ponieważ instalacja każdego z Critical Patch Updates (CPU) na różnych systemach wymaga wiele trudu, wykonaliśmy to zadanie dla Państwa.

W ramach nowego CPU-Info instalujemy CPU na różnych systemach i na różnych wersjach bazy danych Oracle. Do tej pory są to:

Platform	Linux x86-64	Solaris 64 Bit (SPARC)	AIX 5L	Windows AMD 64Windows 2003 R2 SP2 64 Bit
Version	11.2.0.1	11.1.0.7	11.2.0.1	11.1.0.7
	11.1.0.7	10.2.0.4	10.2.0.4	10.2.0.4
	10.2.0.4			

Tabela 2: Przetestowane systemy i wersje baz danych

Instalacje są testowane przez Grid Control zarówno manualnie jak i automatycznie.

Chętnie doradzimy Państwu przy konfiguracji Oracle Grid Control odnośnie automatycznego Patch Deployment lub też innej konfiguracji oprogramowania firmy Oracle.

Jako podstawę do instalacji aktualnego CPU wykorzystujemy zawsze wcześniejsze instalacje CPU (dla aktualnego CPU-Info wykorzystaliśmy CPU z kwietnia 2011).

## 5.2 Wyniki przeprowadzonych testów

Poniżej przedstawiamy zestawienie przedstawiające, który Patch został zainstalowany na jakiej bazie danych oraz jakie wystąpiły problemy w czasie instalacji.

Platforma	Linux x86-64	Linux x86-64	Linux x86-64	Solaris 64 Bit (SPARC)	Solaris 64 Bit (SPARC)
Wersja RDBMS	10.2.0.4	11.1.0.7	11.2.0.1	10.2.0.4	11.1.0.7
Numer Patch	12419249	12419265	12419278	12419249	12419265
Wyniki instalacji ręcznej					
Komentarz do instalacji ręcznej	Automatyczna instalacja działa na poprzedniej wersji CPUApr2011	ORA-29701: unable to connect to Cluster Manager ORA-29701 At Startup Of ASM Instance [ID 459775.1]	Ręczna instalacja działa na poprzedniej wersji CPUApr2011	Ręczna instalacja działa na poprzedniej wersji CPUApr2011	Ręczna instalacja działa na poprzedniej wersji CPUApr2011
Wyniki instalacji automatycznej					
Komentarz do instalacji automatycznej	Automatyczna instalacja działa na poprzedniej wersji CPUApr2011	Automatyczna instalacja działa na poprzedniej wersji CPUApr2011	Automatyczna instalacja działa na poprzedniej wersji CPUApr2011	Automatyczna instalacja działa na poprzedniej wersji CPUApr2011	UTIL session Syntax Error... Unrecognized Option for util, patch napply -id 10426994,1256039 3. - musiała zostać ręcznie wykonana

Tabelle 3a: Wyniki instalacji testowych

Platforma	AIX 5L	AIX 5L	Windows AMD 64Windows 2003 R2 SP2 64 Bit	Windows AMD 64Windows 2003 R2 SP2 64 Bit
Wersja RDBMS	10.2.0.4	11.2.0.1	10.2.0.4	11.1.0.7
Numer Patch	11725015	11724991	12328503	11741170
Wyniki instalacji ręcznej				
Komentarz do instalacji ręcznej	Automatyczna instalacja działa na poprzedniej wersji CPUApr2011	Automatyczna instalacja działa na poprzedniej wersji CPUApr2011	Automatyczna instalacja działa na poprzedniej wersji CPUApr2011	Automatyczna instalacja działa na poprzedniej wersji CPUApr2011
Wyniki instalacji automatycznej				
Komentarz do instalacji automatycznej	Opatch Fails to Replace libjox*.a While Applying One Off Patch on AIX Platform [ID 779083.1]	Automatyczna instalacja działa na poprzedniej wersji CPUApr2011	Automatyczna instalacja działa na poprzedniej wersji CPUApr2011	Automatyczna instalacja działa na poprzedniej wersji CPUApr2011

Tabelle 3b: Wyniki instalacji testowych

#### Legenda:

- = Wykonano pomyślnie, żadne błędy nie wystąpiły.
- = Wykonano pomyślnie, lecz dodatkowe kroki musiały zostać wykonane
- = Błąd. Dany krok nie został wykonany

## 6 Glosariusz

---

Poniższy słownik zawiera krótkie opisy terminów użytych w CPU-Info.

Wszystkie te pojęcia są szczegółowo omawiane podczas „Secure Development Trainings”. Te i inne szkolenia przeprowadzane są regularnie w firmie OPITZ CONSULTING.

**CPU** – oznacza *Critical Patch Updates*, określenie używane przez Oracle na poprawki związane z bezpieczeństwem. Za pomocą zapytania SQL (`select * from dba_registry_history`) można dowiedzieć się, jakie poprawki są zainstalowane w bazie danych.

**CVE** – jest skrótem od „*Common Vulnerabilities and Exposures*”, będącym standardem nazewniczym dla luk w systemie bezpieczeństwa systemów komputerowych.

**DoS** – skrót od „*Denial of Service*” i oznacza formę ataku na serwer albo komputer w sieci powodującą niezdolność do świadczenia danych usług. Z reguły dokonuje się tego przez przeciążenie.

**SQL-Injection** – jest luką w bazie danych, umożliwiającą napastnikowi wywołanie dodatkowych poleceń SQL w celu eskalacji przywilejów albo uzyskania dostępu do nieuprawnionych danych. *SQL-Injection* może wystąpić na wszystkich warstwach oprogramowania (klient, serwer aplikacyjny, baza danych, skrypty bazodanowe). Przyczyną jest zawsze zła walidacja wprowadzanych danych.

**CSRF** – skrót od Cross-Site Request Forgery. Oznacza, że napastnik „podsuwa” ofierze poprzez przeglądarkę swój HTTP-Request, który zostaje następnie wykonany z wykorzystaniem Session ID oraz uprawnień wykorzystanego w ten sposób użytkownika.

**DBCA** – skrót dla Database Configuration Assistant, graiczne narzędzie do konfiguracji baz danych  
**PSU** - oznacza Patch Set Update. PSU jest – analogicznie do CPU – publikowane kwartalnie przez Oracle. PSU obok luk bezpieczeństwa usuwa również istotne błędy funkcjonalne.

## 7 Uwagi prawne

---

**OPITZ CONSULTING** oraz firma Red Database Security przeprowadzają testy w oparciu o instalacje standardowe. Sprawdzenia te przeprowadzone są z wielką starannością przez wykwalifikowanych ekspertów. Nie mogą jednak wykluczyć dodatkowych czynników wpływających na różnice pomiędzy środowiskiem klienta a środowiskiem testowym OPITZ CONSULTING oraz firma Red Database Security nie ponoszą żadnej odpowiedzialności, za szkody powstałe w skutek zainstalowania lub nie zainstalowania poprawek zawartych w Critical Patch Update.