

XI Konferencja PLOUG
Kościelisko
Październik 2005

Biuletyn Bezpieczeństwa PLOUG – Podsumowanie 2005

Wojciech Dworakowski

SecuRing

e-mail: adres@e_mail

Streszczenie

W Biuletynie Polskiej Grupy Użytkowników Systemów Oracle - PLOUG'tki, od prawie trzech lat ukazuje się stała rubryka – Biuletyn Bezpieczeństwa PLOUG. Celem biuletynu jest przybliżanie administratorom nowych podatności w produktach Oracle i wiążących się z nimi zagrożeń. Źródłem dla publikowanych tam informacji są nie tylko dokumenty Oracle ale przede wszystkim źródła niezależne, często związane z badaniami, które wykryły opisywane zagrożenia.

Jak co roku, podczas wykładu zostanie przedstawione podsumowanie Biuletynu Bezpieczeństwa z okresu ostatnich 12 miesięcy. Zostaną przedstawione najważniejsze zagrożenia dla bezpieczeństwa produktów Oracle, które ujrzały światło dzienne w ostatnim roku. Duży nacisk zostanie położony na praktykę administracyjną, tzn. - kiedy dane zagrożenie się uaktywnia, jak wielkie ryzyko wiąże się z danym zagrożeniem, czy istnieje publicznie dostępny exploit, jakie metody dodatkowe i obejścia można zastosować, by ustrzec się przed podobnymi zagrożeniami w przyszłości.

Informacja o autorze

Ekspert ds. bezpieczeństwa IT w firmie SecuRing. Koordynator prac zespołu i osoba odpowiedzialna za sporządzanie raportów. Osiem lat doświadczenia praktycznego w zakresie bezpieczeństwa IT. Od pięciu lat zajmuje się również problemami bezpieczeństwa produktów Oracle. Prelegent na licznych konferencjach poświęconych bezpieczeństwu IT (m.in. CERT Secure, PLOUG, Open Source Security, Windows Security). Prowadzi rubrykę poświęconą bezpieczeństwu w Biuletynie PLOUG. Posiada certyfikat Audytora Wiodącego Systemu Zarządzania Bezpieczeństwem Informacji wg BS 7799.

1. Oracle Critical Patch Update

Najważniejszym wydarzeniem mijającego roku związanym z bezpieczeństwem Oracle było niewątpliwie wdrożenie przez Oracle nowego systemu wypuszczania poprawek. Po początkowym zamieszaniu ostatecznie przyjęto, że poprawki będą wypuszczane zbiorczo, raz na kwartał. Ma to spowodować, że administratorzy nie będą zaskakiwani pojawieniem się poprawki i będą mogli lepiej się przygotować do procesu wdrażania patchy. Kwartalne zbiory poprawek są zbiorcze, co oznacza, że zawierają również poprzednie poprawki. Tak więc przy instalacji nowej bazy wystarczy wgrać tylko ostatni Critical Patch Update. Niestety od tej reguły bywają wyjątki i co najmniej raz zdarzyło się że Oracle zapomniało uwzględnić jednej z poprawek (patrz Ploug'tki 35).

Szczegóły dotyczące wykorzystania błędów są z reguły publikowane przez źródła niezależne tuż po wypuszczeniu Oracle Patch Update. Warto jednak wspomnieć, że Oracle nie spieszy się z poprawianiem wykrywanych błędów. Na stronach badaczy bezpieczeństwa pojawiły się już spisy podatności zgłoszonych i nie poprawionych. Przykładowo:

<http://www.red-database-security.com/portal/content.php?content.7>

<http://www.blackhat.com/presentations/bh-usa-05/bh-us-05-cerrudo.pdf>

Przejrzenie tego typu informacji a zwłaszcza dat zgłoszenia problemu daje pojęcie o tym jakie jest podejście do problemów bezpieczeństwa w korporacji. Powyższy indeks zawiera ponad 30 niezalatanych dziur w produktach Oracle. Niektóre z podatności były zgłoszone ponad 2 lata temu!

2. Przegląd nowych podatności w produktach Oracle

Podatności w produktach Oracle, o których opublikowano informacje w ciągu ostatniego roku było bardzo dużo. W ciągu krótkiego wykładu nie sposób przekazać informacje o wszystkich z nich (zainteresowanych odsyłam do Biuletynu Bezpieczeństwa publikowanego w PLOUG'tkach: <http://www.ploug.org.pl/Ploug'tki.php>). Poniżej krótko przedstawiam najgroźniejsze podatności. Dla lepszej przejrzystości podzieliłem je w zależności od uprawnień początkowych jakie musi posiadać intruz żeby daną podatność wykorzystać.

Ataki z poziomu dowolnego użytkownika bazy danych

W tej grupie są głównie podatności polegające na nadużyciu procedur dostępnych dla grupy PUBLIC. Dla systemu przywilejów bazy Oracle charakterystyczne jest to, że procedura może wykonywać się z uprawnieniami wywołującego lub z uprawnieniami właściciela. Właścicielem wielu procedur dostępnych dla grupy PUBLIC jest DBA lub inny użytkownik o wysokich przywilejach. Wiele z tych procedur wykonuje się z uprawnieniami właściciela i jest dostępna dla grupy PUBLIC. W ciągu ostatniego roku wysiłek poszukiwaczy „dziur” w Oracle skupiał się właśnie na tego typu procedurach a to ze względu na to, że znalezienie „dziury” w takiej procedurze oznacza możliwość wykonania kodu PL/SQL z uprawnieniami DBA. Do tej grupy należą następujące podatności opisane w ostatnim roku:

Błędy typu SQL-injection w procedurach dostępnych dla grupy PUBLIC pozwalają na osiągnięcie przywilejów DBA

W następujących procedurach PL/SQL standardowo dostępnych dla grupy PUBLIC wykryto błędy typu SQL injection:

- ORASSO.WPG_SESSION – funkcja init – właściciel: ORASSO lub PORTAL (w obydwu przypadkach - rola DBA)

- OWF_MGR.WF_EVENT_HTML – funkcja EventQueueDisplay – przywileje OWF_MGR (role SELECT_CATALOG_ROLE i AQ_ADMINISTRATOR)

Funkcje te pozwalają na manipulowanie przekazywanymi do nich parametrami a w rezultacie doklejenie własnego kodu SQL do zapytania wykonywanego przez daną funkcję. Zapytanie intruza jest wykonywane z przywilejami właściciela danego pakietu. W rezultacie pozwala to na wykonanie nieuprawnionego kodu PL/SQL z większymi przywilejami.

Podobne skutki ma wykorzystanie błędów SQL-injection w procedurach z pakietów: DBMS_METADATA, DBMS_CDC_SUBSCRIBE, DBMS_CDC_ISUBSCRIBE, DBMS_CDC_IPUBLISH. Procedury te w wyniku manipulacji parametrami umożliwiają wykonanie funkcji zdefiniowanej uprzednio przez użytkownika. Funkcja ta zostanie wykonana z przywilejami właściciela wyżej wymienionych procedur (w tym wypadku SYS).

Pełny opis: Ploug'tki 34 i 35

Poprawka: Wgranie zbioru poprawek Critical Patch Update – July 2005

Oracle Spatial: Możliwość uzyskania uprawnień DBA w wyniku nadużycia triggerów

Arcyciekawy przykład nadużycia systemu uprawnień Oracle zaprezentował w grudniu 2004 David Litchfield. Błąd został poprawiony już w sierpniu 2004 jednak dopiero w grudniu zostały opublikowane szczegóły jego wykorzystania. Przypadek ten jest o tyle pouczający, że pokazuje jak można wykorzystać zależności pomiędzy różnymi tabelami i procedurami standardowymi dla większości instalacji Oracle.

Trigger SDO_CMT_CBK_TRIG jest uruchamiany przy operacji DELETE na tabeli SDO_TXN_IDX_INSERTS. Trigger ten jest uruchamiany z uprawnieniami MDSYS. Grupa PUBLIC ma m.in. prawa DELETE do tej tabeli, a więc każdy użytkownik może wywołać uruchomienie tego triggera. Trigger SDO_CMT_CBK_TRIG przed właściwym usunięciem danych wykonuje funkcje wymienione w tabelach SDO_CMT_DBK_FN_TABLE i SDO_CMT_CBK_DML_TABLE. Grupa PUBLIC nie ma przywileju INSERT na tych tabelach ale: funkcje CCBKAPPLROWTRIG i EXEC_CBK_FN_DML z pakietu PRVT_CMT_CBK mogą zostać wykorzystane do dopisania nazwy dowolnej procedury do tabel SDO_CMT_DBK_FN_TABLE i SDO_CMT_CBK_DML_TABLE. Funkcje te są dostępne dla grupy PUBLIC ale wykonują się z uprawnieniami MDSYS. W ten sposób dowolny użytkownik może pośrednio dopisać nazwę własnej, wrogiej procedury do tabel SDO_CMT_DBK_FN_TABLE i SDO_CMT_CBK_DML_TABLE a następnie wykonać tą procedurę z prawami MDSYS przez celowe wywołanie triggera obsługującego kasowanie z tabeli SDO_TXN_IDX_INSERTS.

W podobny sposób można wykorzystać również następujące triggerzy:

- MDSYS.SDO_GEOM_TRIG_INS1 wywoływany przy operacji INSERT na tabeli MDSYS.USER_SDO_GEOM_METADATA.
- MDSYS.SDO_LRS_TRIG_INS wywoływany przy operacji INSERT na tabeli MDSYS.USER_SDO_LRS_METADATA.

Pełny opis: Ploug'tki 33.

Poprawka: wgranie poprawek opisanych w Oracle Security Advisory #64

Ataki DoS z poziomu dowolnego użytkownika bazy

Błędy w procedurach dostępnych dla grupy PUBLIC oprócz możliwości wykonania wrogiego kodu PL/SQL z wyższymi przywilejami mogą również skutkować atakiem Denial of Service, czyli np. zablokowaniem motoru bazodanowego. Do tego typu podatności należy zaliczyć:

- Błędy w Oracle Intermedia. Podatne są dwa typy obiektów – ORDImage i ORDDoc. Atak Denial of Service jest wyzwalany przez załadowanie do obiektu odpowiednio skonstruowanego pliku, albo przez odpowiednie ustawienie parametrów obiektu.
- Błędy w pakiecie DBMS_REPCAT_INSTANTIATE. Jedna z procedur z tego pakietu nie sprawdza szczegółowo parametrów przekazywanych w wywołaniu. Na skutek tego, jeśli odpowiedni parametr będzie miał bardzo dużą długość to dojdzie do przepełnienia bufora wejściowego. Skutkiem podania do procedury przypadkowego, długiego ciągu znaków jest zawieszenie serwera, gdyż procesor przy powrocie z procedury przeskoczy do przypadkowego miejsca w pamięci.

Pełny opis: Ploug'tki 34

Poprawka: Wgranie zbioru poprawek Critical Patch Update – July 2005

Ataki z poziomu użytkownika Oracle Forms i Reports

W ostatnim roku widać również spore zainteresowanie badaczy bezpieczeństwa produktami Oracle Forms i Oracle Reports. Na tej platformie jest zbudowana znaczna część aplikacji oraclo-wych oraz same Oracle Applications. Tak więc rozpowszechnienie tego typu błędów jest dość duże. Ryzyko jest tym większe, że aplikacje te z reguły służą do przetwarzania danych dość interesujących dla potencjalnych intruzów.

Możliwość wykonania dowolnego kodu SQL przez dowolną aplikację Oracle Forms

Jeden z badaczy bezpieczeństwa Oracle przypomniał szerokiej publiczności o zapomnianej funkcjonalności „Query/Where” w Oracle Forms. Funkcjonalność ta polega na tym, że jeśli w dowolne pole formatki w trybie zadawania zapytań wpisze się znak dwukropka, to klient Forms pokaże okienko umożliwiające wpisanie zaawansowanej klauzuli WHERE. Właściwość tą intruz może wykorzystać do zadania do bazy dowolnego zapytania (np. poprzez wywołanie podzapytania SQL) albo do wywołania procedury PL/SQL. Wyniki działań intruz można wysłać na swój serwer korzystając np. z procedury utl_http.request.

Pełen opis: Ploug'tki 34

Poprawka: Ustawienie parametru: FORMSxx_RESTRICT_ENTER_QUERY=true

Oracle Forms i Oracle Reports pozwalają na uruchamianie komend systemowych

Znowu nie jest to klasyczna „dziura” lecz raczej niezbyt rozważnie zaprojektowana funkcjonalność. Otóż pliki wykonywalne formatek (*.fmx) i raportów (*.rep, *.rdf) mogą zawierać wywołania komend systemowych. Formatki i raporty są uruchamiane przez odpowiedni proces, zawsze z prawami właściciela instalacji Oracle (na Windows – LOCAL SYSTEM, na unixach – „oracle”). W wywołaniu HTTP Oracle Forms i Oracle Reports jest możliwość podania ścieżki bezwzględnej do pliku wykonywalnego formatki lub raportu (odpowiednio parametry „form/module” i „report”). W związku z powyższym jeśli intruz ma możliwość załadowania przygotowanego przez siebie pliku fmx, rep lub rdf na serwer (np. do własnego katalogu domowego lub do katalogu tymczasowego), to będzie mógł go wykonać w środowisku Forms/Reports z większymi uprawnieniami.

Pełen opis: Ploug'tki 35

Poprawka: Jak dotąd Oracle nie opublikowało poprawki pomimo tego, że błąd został zgłoszony już 2003 roku. Obejściem problemu może być uniemożliwienie użytkownikom ładowania własnych plików na serwer. Jeśli funkcjonalność taka jest jednak konieczna, to można zastosować dodatkowe środki ochronne:

- W Oracle Forms 10g można zablokować możliwość podawania własnych parametrów form/module w URL, poprzez wpis w pliku formsweb.cfg: restrictedURLparams=form,module.
- Za pomocą mod_rewrite w Oracle HTTP Serwer należy zablokować wywołania URL zawierające parametry form, module, report, oraz ścieżkę do pliku, np: "form=..", "module=..", "form=/", "module="/ , "form=c:\", "module=c:\", itd.

Inne błędy w Oracle Forms/Reports

- Błędy w Oracle Reports pozwala na odczytanie części informacji z plików lub nadpisanie plików na serwerze. (Ploug'tki 35)
- Oracle Forms w pewnych warunkach buforuje dane pozyskane z bazy w plikach do odczytu dla wszystkich (Ploug'tki 35)

Ataki na Oracle Application Server

Zdalne wywoływanie dowolnych procedur PL/SQL przez mod_plsql

Błąd dotyczy instalacji Oracle Application Server, które udostępniają aplikację przez Oracle PL/SQL Gateway (mod_plsql). Oracle iAS posiada zabezpieczenia uniemożliwiające bezpośrednie wywoływanie większości standardowych procedur przez bezpośrednie wywołanie URL (np. http://server/pls/dad/SYS.OWA_UTIL.CELLSPRINT?P_THEQUERY=ZAPYTANIE_SQL).

Okazało się że w wersji 10g Application Servera zabezpieczenie to można obejść wykorzystując różne sposoby kodowania znaków w serwerze aplikacji i współpracującej z nim bazy. Przeprowadzenie ataków wymaga eksperymentów, gdyż zależy od kombinacji stron kodowych skonfigurowanych na warstwie serwera aplikacji i bazy danych.

Pełny opis: Ploug'tki 33.

Poprawka: wgranie poprawek opisanych w Oracle Security Advisory #64

Oracle Webcache umożliwia obejście reguł filtrowania URL zdefiniowanych na serwerze WWW

Odwołując się bezpośrednio do portu TCP Oracle Web Cache intruz może dostać się do URL, które są zablokowane przy standardowym dostępie przez serwer WWW (OHS). Przykładowo: /dmsoc4j, /server-status, /dms0. Te ścieżki URL są filtrowane na OHS za pomocą regułek mod_access. Regułki te nie mają zastosowania jeśli odwołanie następuje przez WebCache. A więc żeby się do nich dostać wystarczy wywołać „zakazane” URLe przez port TCP WebCache.

Pełny opis: Ploug'tki 34

Poprawka: W httpd.conf należy ustawić parametr „UseWebCacheIP ON”.

Ataki na E-Business Suite

Oprócz możliwości wykorzystania ataków na środowisko na którym działa E-Business Suite (baza, Application Server, Forms), w ostatnim roku wykryto kilka poważnych błędów charakterystycznych dla samych aplikacji E-Business Suite. W większości są to błędy typu SQL injection umożliwiające kodu SQL w bazie danych z uprawnieniami użytkownika APPS. Na szczęście nie opublikowano szczegółów technicznych dotyczących tych błędów.

Pełny opis: Ploug'tki 34

Poprawka: Wgranie zbioru poprawek Critical Patch Update – July 2005