

X Konferencja PLOUG  
Kościelisko  
Październik 2004

# Biuletyn Bezpieczeństwa PLOUG Podsumowanie 2004

Wojciech Dworakowski

*SecuRing*  
*e-mail: wojtekd@securing.pl*

## **Abstrakt**

W Biuletynie Polskiej Grupy Użytkowników Systemów Oracle – PLOUG’tki, od blisko dwóch lat ukazuje się stała rubryka – Biuletyn Bezpieczeństwa PLOUG. Celem biuletynu jest przybliżanie administratorom zagrożeń związanych z produktami Oracle, które zostały ujawnione w ostatnich miesiącach. Podczas wykładu zostaną przedstawione najważniejsze zagrożenia dla bezpieczeństwa produktów Oracle, które ujrzały światło dzienne w ostatnim roku. Zostaną omówione podatności wiążące się z najważniejszymi zagrożeniami. Dla każdego omawianego zagrożenia zostaną opisane warunki w jakich dana podatność może zostać wykorzystana. Zostaną również omówione liczne podatności ujawnione przez Oracle w sierpniu 2004 w Oracle Security Alert #68, który wzbudził dużo kontrowersji wśród administratorów.



## Kilka uwag na temat uaktualniania

Powszechnie znaną prawdą jest, że aby utrzymać należyty poziom bezpieczeństwa systemu informatycznego, należy regularnie wgrywać uaktualnienia publikowane przez producentów. Z drugiej strony – administratorzy Oracle wiedzą bardzo dobrze o tym, że wgranie uaktualnienia może w różnych specyficznych przypadkach spowodować destabilizację instalacji a nawet konieczność przeinstalowania wszystkiego od zera. Producent również nie pomaga w tym ciężkim zadaniu, bo przy niektórych poprawkach (np. Oracle Security Alert #68) nakazuje restart serwera. Nie zawsze jest to akceptowalne. Naturalnie należy stosować zasadę złotego środka – wgrywać tylko przetestowane i absolutnie niezbędne poprawki. Ale jak określić które uaktualnienia są niezbędne? Producenci z reguły udostępniają bardzo mało szczegółów technicznych na temat podatności łatanych przez poprawki i zalecają wgrywanie każdego uaktualnienia. Oczywiście jest to zalecane, ale szczegółowe testowanie każdej poprawki wiąże się z dużą ilością czasu jaki musi poświęcić administrator a jak wiadomo – czas to pieniądz. Poza tym nawet jeśli mamy osobny system testowy, to przetestowanie na nim poprawki nie gwarantuje nam w 100% że zadziała ona w środowisku produkcyjnym. Tak więc w tym kontekście kluczowa staje ocena czy lepiej mieć niezalany system czy lepiej jest podjąć „ryzyko” wgrania poprawki? Biuletyn Bezpieczeństwa PLOUG ma na celu informowanie o zagrożeniach w możliwie wyczerpujący sposób, tak żeby ułatwić administratorom właściwą ocenę sytuacji i podjęcie decyzji.

Biuletyn Bezpieczeństwa ukazuje się co kwartał w PLOUG-tekach od końca 2002 roku (od numeru 24). Od sierpnia 2004, informacje o podatnościach są również na bieżąco publikowane na serwisie [www.ploug.org.pl](http://www.ploug.org.pl). Poniżej przedstawiam omówienie najgroźniejszych podatności jakie wyszły na jaw w produktach Oracle przez ostatni rok.

## Przegląd nowych podatności w produktach Oracle

### Podatności typu SQL-injection w Oracle 9i Application Server Portal I w E-Business Suite

SQL-injection jest jedną z najczęściej stosowanych metod atakowania aplikacji webowych. Atak SQL-injection polega na doklejeniu do parametrów do zapytania, które jest konstruowane przez wpisanie do formularza HTML danych. Podatność pozwalająca na wykorzystanie tej metody ataku wiąże się z tym, że dane pobierane od użytkownika:

1. są bezpośrednio wklejane do zapytania SQL
2. nie są szczegółowo sprawdzane

Skutkiem ataku SQL-injection jest wykonanie dodatkowego kodu SQL, a więc wiążą się one z reguły z bardzo dużymi zagrożeniami. Dokładniej ta klasa ataków została opisana w artykule „Ataki SQL-Injection czyli firewall i bezpieczna baza danych, to nie wszystko” w 24 numerze PLOUGtek.

Oracle Portal i E-Business suite, to nic innego jak specyficzne aplikacje webowe, a więc mogą być one podatne na tego typu ataki. W ostatnim roku ujawniono podatności typu SQL-injection w modułach PL/SQL, które mogą być udostępniane przez Oracle Portal. Podatności te dotyczą wg producenta następujących modułów:

- Portal DB Provider Forms,
- Portal DB Provider Hierarchy,
- Portal DB Provider XML Components
- List of Values (LOV).

Powyższe moduły są absolutnie kluczowe dla Application Servera i nie mogą być usunięte. Jeśli w eksploatowanej instalacji powyższe moduły są udostępniane (dotyczy to większości przypadków wykorzystania Oracle Portal), to w większości przypadków atakujący może wykonać swój kod SQL w bazie, z uprawnieniami SYS albo SYSTEM. Warto przy tym zaznaczyć, że w standardowej instalacji 9iAS umożliwia użytkownikom „webowym”, bez żadnego uwierzytelnienia, dostęp do pakietów i procedur PL/SQL przechowywanych w bazie. Fakt ten może zostać wykorzystany do zaatakowania bazy podpiętej pod 9iAS pomimo braku udostępniania Oracle Portal.

Podobne podatności odkryto w Oracle E-Business Suite (Oracle Applications). W tym wypadku autor nie ujawnił szczegółów. Wiadomo tylko, że:

- podatności ujawniają się w każdej instalacji dowolnego modułu Oracle Applications
- do przeprowadzenia ataku wystarczy przeglądarka WWW i dostęp do serwera WWW udostępniającego Oracle Applications (bez konieczności posiadania konta w systemie)

**Jedynym sposobem usunięcia opisywanych podatności jest wgranie poprawek.** Zalecałbym to zwłaszcza administratorom Oracle 9iAS, gdyż zostały udostępnione wystarczające szczegóły techniczne do odtworzenia ataku. Podatności dotyczące Oracle Applications są cięższe do wykorzystania, ale dla sprawnego intruza zidentyfikowanie ich nie powinno stanowić większego problemu. Podatne wersje i numery odpowiednich poprawek są podane w Oracle Security Alert nr 61 i 67

## **Błąd w dokumentacji dotyczącej formularza logowania Oracle Single Sign-on**

Oracle Single Sign-on – moduł służący do uwierzytelniania się do wielu usług za pomocą jednokrotnego podania hasła zawiera formularz logowania się przez Web. Formularz ten jest z reguły dostosowywany do potrzeb konkretnej aplikacji. Sposób dostosowania jest opisany w dokumentacji „Oracle 9iAS Single Sign-on Administrators Guide, Release 2(9.0.2)”. Przykład podany w dokumentacji jest często kopiowany i stosowany w praktyce. Niestety – ten przykład zawiera błąd logiczny pozwalający na przechwytywanie haseł użytkowników przez intruza.

Jeśli w eksploatowanej instalacji Oracle Single Sign-on jest stosowany fragment kodu z dokumentacji Oracle, to należy zastosować obejście problemu zaproponowane przez Oracle. Polega ono na zakodowaniu adresu strony odpowiadającej za uwierzytelnienie, na stałe, w kodzie formatki logowania w zmiennej `p_submit_url`.

Błąd występuje tylko w instalacjach, w których zastosowano fragment kodu z dokumentacji, jednak skutki tej podatności są na tyle groźne, że warto sprawdzić swoje instalacje Oracle SSO.

Więcej szczegółów: <http://www.madison-gurkha.com/advisories/MG-2004-01.txt>

## **Liczne błędy ujawnione w sierpniu 2004 (OSA #68)**

27.07.2004, na konferencji Blackhat Briefings, znany badacz bezpieczeństwa David Litchfield oświadczył podczas swojej prezentacji, że w obecnie eksploatowanych wersjach Oracle istnieje 34 nowe podatności, w tym podatności o znaczeniu kluczowym, umożliwiające przejście kontroli nad bazą bez żadnych początkowych uprawnień. Litchfield powiedział, że poinformował Oracle o podatnościach już w styczniu tego roku. W maju uzyskał informacje, że korporacja przygotowała poprawki jednak nie udostępnia ich ze względu na... nowe zasady publikowania poprawek nad którym pracuje firma Oracle.

Pomimo licznych publikacji w prasie informatycznej krytykujących postawę Oracle, poprawki ukazały się dopiero 31.08.2004. Wtedy też ukazał się Oracle Security Alert nr 64 zatytułowany po prostu „Oracle Security Update”. Informacja o błędach jest dość lakoniczna i nie pozwala na pełne przeanalizowanie podatności i stwierdzenie czy faktycznie jest konieczne wgranie poprawek w konkretnej instalacji bazy. Na dodatek – instalacja poprawek wymaga restartu bazy co nie zawsze jest proste w instalacjach wymagających wysokiej dostępności. Nic dziwnego – podobno „pacz-

ka”, której instalacje zaleca Oracle zawiera ponad 100 poprawek dotyczących bezpieczeństwa! ([http://www.theregister.co.uk/2004/09/02/oracle\\_patch\\_tsunami/](http://www.theregister.co.uk/2004/09/02/oracle_patch_tsunami/))

Na szczęście część precyzyjniejszych informacji jest dostępna w źródłach niezależnych – na stronach związanych z odkrywcami podatności. Spróbujmy podsumować dostępne informacje.

Firma Application Security Inc. udostępniła uaktualnienia do swojego skanera bezpieczeństwa AppDetective for Oracle: (<http://www.appsecinc.com/resources/alerts/oracle/2004-0001/>) W opisach szczegółowych można znaleźć informacje o 44 procedurach Oracle, które są podatne na ataki buffer overflow. Informacje są dość precyzyjne, więc doświadczony intruz może stosunkowo szybko stworzyć kod wykorzystujący te podatności (exploit). Należy przypuszczać że exploity dotyczące tych podatności krążą w „podziemiu”. Kilka z podatnych procedur jest dostępnych dla grupy PUBLIC, a więc dziury w nich obecne mogą zostać wykorzystane przez każdego użytkownika bazy. Skutkiem ataku jest wykonanie dowolnego kodu w systemie operacyjnym z uprawnieniami użytkownika „oracle” (lub użytkownika z którego uprawnieniami działa Oracle w systemie operacyjnym).

Firma Davida Litchfielda – Next Generation Security Software opublikowała okrojone informacje o błędach wykrytych przez nich, ale zapowiedziała, że wszystkie szczegóły ujawnią 31.11.2004 (<http://www.nextgenss.com/advisories/oracle-01.txt>), po trzech miesiącach karencji jaką dają administratorom na załatwienie systemów. Wiadomo jedynie, że podatności dotyczą możliwości doklejania swojego kodu do parametrów procedur PL/SQL (SQL-injection), manipulacji triggerami, błędów w procedurach konwersji znaków i możliwości ataków denial of service (ataki których celem jest obniżenie dostępności systemu). Wiadomo również że część podatności może być wykorzystana przez intruza nie posiadającego nawet konta w bazie i że są one stosunkowo łatwe do wykorzystania.

Peter Finnigan poinformował o podatności w nowej funkcjonalności dodanej w Oracle 10g ([http://www.petefinnigan.com/dbms\\_scheduler.pdf](http://www.petefinnigan.com/dbms_scheduler.pdf)). Podatność dotyczy nowego pakietu DBMS SCHEDULER, która umożliwi wykonywanie zadań (w tym komend systemu operacyjnego) przez użytkowników z przywilejem CREATE JOB. Według zamieszczonej informacji, pakiet ten może zostać wykorzystany do zdobycia przywilejów DBA i zdobycia dostępu do systemu operacyjnego. Autor jako obejście problemu zaleca odebranie dostępu do DBMS SCHEDULER grupie PUBLIC i odebranie wszystkim użytkownikom przywileju CREATE JOB.

Na stronach firmy Red Database Security (<http://www.red-database-security.com/>) można wytropić informacje o trzech kolejnych podatnościach. Dwie z nich umożliwiają ataki metodą buffer overflow i można je wykorzystać w specyficznych warunkach. Natomiast trzecia podatność jest dużo groźniejsza i łatwiejsza do wykorzystania. Według zamieszczonych informacji, jeśli jest zainstalowany moduł CTXSYS, to dowolny użytkownik bazy może osiągnąć przywileje DBA przez wykonanie pakietu DRILOAD i przekazanie odpowiednich parametrów. Funkcja driload.validate\_stmt umożliwia wykonanie dowolnego kodu SQL jako użytkownik CTXSYS (czyli DBA)! Problem wynika z tego, że:

- Pakiet CTXSYS.DRILOAD jest udostępnione dla grupy PUBLIC
- Pakiet ten używa uprawnień właściciela (czyli konta CTXSYS) zamiast uprawnień wywołującego
- Pakiet CTXSYS.DRILOAD wykonuje dowolną komendę SQL bez żadnego sprawdzania

Podatne są wszystkie wersje bazy do 9.2.0.4 włącznie. Nie jest jasne czy jest podatne 10gR1. Obejście problemu polega na odebraniu przywilejów do pakietu CTXSYS.DRILOAD (o ile nie jest wykorzystywany) lub usunięciu (zablokowanie nie wystarczy) konta CTXSYS.

Podsumowując:

- Obecnie ryzyko ataku na bazę z zewnątrz, bez posiadania konta w systemie nie jest bardzo duże. Podatności pozwalające na taki atak istnieją jednak nie zostały udostępnione żadne szczegóły pozwalające na ich wykorzystanie. Można jednak przypuszczać, że odpowiednie exploity krążą w środowisku hackerów.

- Ryzyko związane z działalnością intruza posiadającego uprawnienia typowego użytkownika bazy należy uznać za duże. Opublikowane szczegóły są wystarczające do skonstruowania ataku przez średnio-zaawansowanego intruza.
- Szczególną uwagę należy zwrócić na aplikacje internetowe korzystające z bazy Oracle. Mnogość podatności wykrytych w różnych funkcjach bazy może prowadzić do możliwości wykorzystania niektórych z nich w kontekście aplikacji webowej, przez atak z zewnątrz. Atakom tego typu można zaradzić stosując szczegółowe sprawdzanie zmiennych pobieranych od użytkownika i przekazywanych jako parametry do wywołań procedur bazy danych.
- Po 31.11.2004 zagrożenie może znacznie wzrosnąć. Tego dnia David Litchfield zapowiedział opublikowanie szczegółów odkrytych przez niego podatności.