

Oracle SYS.DBMS_AQADM_SYS – Privilege Elevation Vulnerability

Background

Oracle is a widely deployed DBMS that contains various built-in packages. The DBMS_AQADM package provides procedures to manage Oracle Streams Advanced Queuing (AQ) configuration and administration information. DBMS_AQADM_SYS is a package used internally by DBMS_AQADM to implement some of its functionality. This package contains an EXECUTE_STMT procedure.

Scope

Imperva's Application Defense Center is conducting an extensive research of the Oracle DBMS and Oracle packages. As part of the research the team has identified a privilege elevation vulnerability in the DBMS_AQADM_SYS package.

Findings

An attacker can use the DBMS_AQADM_SYS.EXECUTE_STMT procedure to execute an arbitrary SQL query with the security content of a higher privileged user.

Details

When calling DBMS_AQADM_SYS.EXECUTE_STMT procedure with custom SQL query as an argument, the query is executed as-is with the security privileges of the SYS user. The call can be performed by any user that has "execute" privilege on the DBMS_AQADM_SYS package.

Exploit

The following code demonstrates a way to exploit the vulnerability:

```
begin
  sys.dbms_aqadm_sys.execute_stmt('grant dba to scott');
end;
```

Tested Versions

Oracle Database 11.1.0.6

Vulnerable

Oracle Database 11.1.0.6

Not Vulnerable

Vendor's Status

Vendor notified on Apr-19-09.

Fixed in future releases

Workaround

Disable access to the DBMS_AQADM_SYS package.

Discovered By

Yaniv Azaria of Imperva's ADC