

Oracle SYS.DBMS_AQADM – 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. This package contains a SET_SESSION_EVENT procedure that receives two arguments.

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 package.

Findings

An attacker can use the DBMS_AQADM.SET_SESSION_EVENT procedure to execute an alter session statement with the security context SYS.

Details

When calling DBMS_AQADM.SET_SESSION_EVENT procedure, an "alter session set events ..." statement is executed as the database user SYS, where the statement itself is constructed with non-sanitized arguments. Thus, a malicious user can append arbitrary set clauses to the statement.

Exploit

The following code alters the events parameter and enable SQL trace for the session:

```
begin
  sys.dbms_aqadm.set_session_event('immediate trace name treedump level 1' sql_trace
  = true --', '0');
end;
```

Tested Versions

Vulnerable

Oracle Database 11.1.0.6

Not Vulnerable

Vendor's Status

Vendor notified on Apr-19-09.

Fixed in Oracle 11.2

Workaround

Disable access to the DBMS_AQADM package.

Discovered By

Yaniv Azaria of Imperva's ADC