PL/SQL static code analysis: Sensitive "SYS" owned functions should not be used

1-2 minutes

Some Oracle packages contain powerful SYS-owned functions that can be used to perform malicious operations. For instance, `DBMS_SYS_SQL.PARSE_AS_USER` can be used to execute a statement as another user.

Most programs do not need those functions and this rule helps identify them in order to prevent security risks.

Noncompliant Code Example

```
DECLARE
  c INTEGER;
  sqltext VARCHAR2(100) := 'ALTER USER system IDENTIFIED BY hacker'; -- Might be injected by the user
BEGIN
  c := SYS.DBMS_SYS_SQL.OPEN_CURSOR();
-- Noncompliant

   -- Will change 'system' user's password to 'hacker'
  SYS.DBMS_SYS_SQL.PARSE_AS_USER(c, sqltext, DBMS_SQL.NATIVE, UID);  -- Non-Compliant
```

```
  SYS.DBMS_SYS_SQL.CLOSE_CURSOR(c);
-- Noncompliant
END;
/
```

See

- MITRE, CWE-269 - Improper Privilege Management
- MITRE, CWE-270 - Privilege Context Switching Error