

# DRD04-J. Do not log sensitive information

Android provides capabilities for an app to output logging information and obtain log output. Applications can send information to log output using the `android.util.Log` class. To obtain log output, applications can execute the `logcat` command.

## To log output

The `android.util.Log` class allows a number of possibilities:

<code>Log.d (Debug)</code>	<code>Log.e (Error)</code>	
<code>Log.i (Info)</code>	<code>Log.v (Verbose)</code>	<code>Log.w (Warn)</code>

### Example:

```
Log.v("method", Login.TAG + ", account=" + str1);
Log.v("method", Login.TAG + ", password=" + str2);
```

## To obtain log output

Declare `READ_LOGS` permission in the manifest file so that an app can read log output:

AndroidManifest.xml:

```
<uses-permission android:name="android.permission.READ_LOGS" />
```

Call `logcat` from an application:

```
Process mProc = Runtime.getRuntime().exec(
    new String[]{"logcat", "-d", "method:V *:S$Bc`W^(B)"});

BufferedReader mReader = new BufferedReader(
    new InputStreamReader(proc.getInputStream()));
```

Prior to Android 4.0, any application with `READ_LOGS` permission could obtain all the other applications' log output. After Android 4.1, the specification of `READ_LOGS` permission has been changed. Even applications with `READ_LOGS` permission cannot obtain log output from other applications.

However, by connecting an Android device to a PC, log output from other applications can be obtained.

Therefore, it is important that applications do not send sensitive information to log output.

## Noncompliant Code Example

Facebook SDK for Android contained the following code which sends Facebook access tokens to log output in plain text format.

```
Log.d("Facebook-authorize", "Login Success! access_token="
    + getAccessToken() + " expires="
    + getAccessExpires());
```

Source: <http://blog.parse.com/2012/04/10/discovering-a-major-security-hole-in-facebooks-android-sdk/>

## Noncompliant Code Example

Here is another example. A weather report for Android sent a user's location data to the log output as follows:

```
//MyWeatherReport( 6483): Re-use MyWeatherReport data
// ( 6483): GET JSON: http://example.com/smart/repo_piece.cgi?arc=0&lat=26.209026&lon=127.
650803&rad=50&dir=-999&lim=52&category=1000
```

If a user is using Android OS 4.0 or before, other applications with `READ_LOGS` permission can obtain the user's location information without declaring `ACCESS_FINE_LOCATION` permission in the manifest file.

## Proof of Concept

Example code of obtaining log output from a vulnerable application is as follows:

```
final StringBuilder slog = new StringBuilder();

try {
    Process mLogcatProc;
    mLogcatProc = Runtime.getRuntime().exec(new String[]
        {"logcat", "-d", "LoginAsyncTask:I APIClient:I method:V *:S" });

    BufferedReader reader = new BufferedReader(new InputStreamReader(
        mLogcatProc.getInputStream()));

    String line;
    String separator = System.getProperty("line.separator");

    while ((line = reader.readLine()) != null) {
        slog.append(line);
        slog.append(separator);
    }
    Toast.makeText(this, "Obtained log information", Toast.LENGTH_SHORT).show();

} catch (IOException e) {
    // handle error
}

TextView tView = (TextView) findViewById(R.id.logView);
tView.setText(slog);
```

## Applicability

Applications should make sure that they do not send sensitive information to log output. If the app includes a third party library, the developer should make sure that the library does not send sensitive information to log output. One common solution is for an application to declare and use a custom log class, so that log output is automatically turned on/off based on Debug/Release. Developers can use ProGuard to delete specific method calls. This assumes that the method contains no side effects.

This rule is a special case of [FIO13-J. Do not log sensitive information outside a trust boundary.](#)

## Risk Assessment

Logging sensitive information can leak sensitive information to malicious apps.

Rule	Severity	Likelihood	Remediation Cost	Priority	Level
DRD04-J	Medium	Probable	Medium	P8	L2

## Automated Detection

Automatic detection of the use of logging facilities trivial. It is not feasible to automatically determine whether the data being logged is sensitive.

## Related Vulnerabilities

- Facebook SDK for Android: <http://readwrite.com/2012/04/10/what-developers-and-users-can#awesm=-o9iqZAMIUPshPu>
- [JVN#23328321](#) Puella Magi Madoka Magica iP for Android vulnerable to information disclosure
- [JVN#86040029](#) Weathernews Touch for Android stores location information in the system log file
- [JVN#33159152](#) Loctouch for Android information management vulnerability
- [JVN#56923652](#) Monaca Debugger for Android information management vulnerability

## Related Guidelines

## Bibliography

[JSSEC 2014] 4.8 Outputting log to LogCat

