

**Oracle Security Alert #47**  
**Dated: 19 December 2002**  
**Severity: 3**

**Security Vulnerabilities in Oracle 9i Application Server**

This note describes three potential security vulnerabilities in Oracle9i Application Server.

**Description**

1. Java Server Pages (JSPs) were vulnerable to source code disclosure.
2. Default permissions when Oracle9i Application Server was installed allowed Everyone/Full Control access to files.
3. Contents of the WEB-INF folder (for OC4J) were accessible.

---

**1. Description**

Java Server Pages (JSPs) were vulnerable to source code disclosure.

**Products affected**

Oracle9i Application Server Release 2 v. 9.0.2.0.0

**Platforms affected**

All Platforms

**Upgrade Information**

This is fixed in Oracle9i Application Server Release 2 v. 9.0.2.0.1 on all platforms.

---

**2. Description**

Default permissions when Oracle9i Application Server was installed allowed Everyone/Full Control access to files.

**Products affected**

Oracle9i Application Server v. 1.0.2.2

**Platforms affected**

Windows (NT, 2000)

**Upgrade Information**

This is fixed in Oracle9i Application Server Release 2 v. 9.0.2.0.1 on all platforms.

**Workaround**

If the file system is NTFS, allow members of the Administrator group full control of the Oracle home directory and all subdirectories. Set permissions so that other users have no access to these directories at all.

---

**3. Description**

Contents of the WEB-INF folder (for OC4J) were accessible.

**Products affected**

Oracle9i Application Server v. 1.0.2.2, and Release 2, v. 9.0.2.0.0 and v. 9.0.2.0.1

**Platforms affected**

All Platforms

**Upgrade Information**

This is fixed in v. 9.0.2.0.1 on NT, and is fixed in v. 9.0.3 for Solaris and other Unix platforms.

**Workaround**

For Unix platforms using v. 9.0.2.0.0 and 9.0.2.0.1, a workaround is described in Alert 28. This workaround is also documented in the product release notes for v. 9.0.2.0.1.

---

**Credits**

Oracle Corporation thanks Matt Moore of Westpoint Ltd. for discovering and bringing these potential security vulnerabilities to Oracle's attention.