Oracle Security Alert 47
Dated: 19 December 2002
Updated: 23 July 2003
Severity: 3

Security Vulnerabilities in Default Installation of Oracle9*i* Application Server
This note describes three potential security vulnerabilities in Oracle9i Application Server:

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

Issue 1. Description
Java Server Pages (JSPs) are 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 potential vulnerability is fixed in Oracle9*i* Application Server Release 2, v 9.0.2.0.1 and onwards on all platforms.

Issue 2. Description
Default permissions on installed Oracle9*i* Application Server allow Everyone/Full Control access to files.

Products affected
Oracle9*i* Application Server Release 1, v 1.0.2.2

Platforms affected
Windows (NT, 2000)

Upgrade Information
This potential vulnerability is fixed in Oracle9*i* Application Server Release 2, v 9.0.2.0.1 and onwards 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. Revoke all other permissions from all other users.

Issue 3. Description
Contents of the WEB-INF folder (for OC4J) are accessible by default.

Products affected
Oracle9*i* Application Server Release 1, 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 potential vulnerability is fixed in Oracle9*i* Application Server Release 2, v 9.0.2.0.1 on Windows (NT/2000), and in Oracle9*i* Application Server Release 2, v 9.0.3 for Solaris and other Unix platforms.

Workaround
For customers running v 9.0.2.0.0 and v 9.0.2.0.1 on Unix platforms, a workaround is described in Oracle Security Alert 28, http://otn.oracle.com/deploy/security/pdf/ias_modplsql_alert.pdf. This workaround is also documented in the product release notes for v 9.0.2.0.1.

Special Note for E-Business Suite 11*i*

The Oracle E-Business Suite11*i* uses several components delivered as part of the Oracle9*i* Application Server Release 1 (v 1.0 and v 1.0.2.2). Oracle E-Business Suite 11*i* customers may be impacted by the security alerts issued for v 1.0.2.2. If you are an Oracle E-Business Suite 11*i* customer, please make sure that you have applied the latest ROLLUP PATCH for Oracle9*i* Application Server Release 1, v 1.0.2.2 & Oracle E-Business Suite 11*i* as mentioned in the document entitled "Installing Oracle9i Application Server with Oracle E-Business Suite 11*i*", (Metalink Note 146468.1).

Credits

Oracle Corporation thanks Matt Moore of Pentest Ltd. and David Litchfield, of Next Generation Security Software Ltd., for discovering and bringing these potential security vulnerabilities to Oracle's attention. The Next Generation Security Software Advisory is available at http://www.nextgenss.com/research/advisories.html.

Modification History

19-DEC-02: Initial release, Version 1
19-MAY-03: Minor updates to flow of textual descriptions
23-JUL-03: Re-released with E-Business Suite information, Version 5