Oracle Security Alert 65
Updated: 2 June 2004
Severity: 2

Security Vulnerability in Oracle9*i* Application and Database Servers

Description

A potential security vulnerability has been discovered in Oracle9*i* Application Server and Oracle9*i* Database Server. The vulnerability involves the processing of SOAP (Simple Object Access Protocol) messages whose XML contains carefully constructed Data Type Definitions (DTDs). Note that SOAP is the basis of Web Services that are therefore also affected.

Supported Products Affected

- Oracle9*i* Application Server Release 2, version 9.0.3.0 and 9.0.3.1
- Oracle9*i* Application Server Release 2, version 9.0.2.3 and earlier versions
- Oracle9*i* Application Server Release 1, versions 1.0.2.2 and 1.0.2.2.2
- Oracle9*i* Database Server Release 2, versions 9.2.0.1 and later

E-Business Suite 11i Customers

Oracle E-Business Suite Release 11*i* customers must apply patches listed in the "Patch Availability Matrix" as they correspond to their current Oracle 9*i* Application Server or Oracle 9i Database Server releases listed below:

- Oracle 9*i* Application Server Release 1, version 1.0.2.2.2
- Oracle 9*i* Database Server Release 2, version 9.2.0.2

Platforms Affected

All

Required Conditions for Exploit

Access to SOAP enabled servers. Both XML and SOAP are installed by default in Oracle9*i* Application Server and Oracle9*i* Database Server when the Oracle HTTP Server is installed.

Risk to Exposure

Risk to exposure is high in Oracle9*i* Application Server Release 2, version 9.0.2.1 and earlier because authentication to SOAP is not turned on by default. However, risk to exposure is moderate in post-Oracle9*i* Application Server Release 2, version 9.0.2.1 and in Oracle9*i* Database Server because authentication to SOAP is required. A knowledgeable and malicious user can exploit this vulnerability to cause a Denial of Service (DoS) against Oracle9*i* Application Server and Oracle9*i* Database Server.

How to Minimize Risk

If SOAP is protected by client authentication before the processing of SOAP XML data structures, unauthenticated clients do not pose a threat; for example, SSL sessions

protected by Client X.509 certificates are protected against unauthenticated clients.

For those sites that do not use SOAP, disabling SOAP is a workaround. Disable SOAP by removing or renaming the following SOAP library, which is delivered in the following JAR file:

```
[Oracle Home]/soap/lib/soap.jar
```

Removing or renaming this library will remove access to SOAP, including support for Web services functionality.

Ramification for Customer

Customers are vulnerable unless the workaround or patch is applied. Oracle strongly recommends that customers review the severity rating for this Alert and patch accordingly. See

http://otn.oracle.com/deploy/security/pdf/oracle_severity_ratings.pdf

for a definition of severity ratings.

Patch Availability

Please see Metalink Document ID 259556.1:

http://metalink.oracle.com/metalink/plsql/ml2_documents.showDocument?p_database_id=NOT&p_id=259556.1

for the patch download procedures and for the **Patch Availability Matrix** for this Oracle Security Alert.

Oracle strongly recommends that you backup and comprehensively test the stability of your system upon application of any patch prior to deleting any of the original file(s) that are replaced by the patch.

Credits

Oracle Corporation thanks Amit Klein of Sanctum Inc. for discovering and promptly bringing this potential security vulnerability to Oracle's attention.

Modification History

18-FEB-04: Initial release, Version 1
12-MAR-04: Added EBS statement; clarified affected product list, Version 2
16-APR-04: Modified Product Affected section, Version 3
02-JUN-04: Removed generic patch wording, Version 4