Oracle Security Alert 64
Dated: 18 February 2004
Updated: 20 May 2004
Severity: 2

Security Vulnerabilities in Oracle9*i* Database Server

Description
Security vulnerabilities have been discovered in Oracle9*i* Database Server Release 1 and Release 2.

Supported Products Affected
- Oracle9*i* Database Server Release 2, 9.2.0.4 and 9.2.0.3
- Oracle9*i* Database Server Release 1, 9.0.1.4 and 9.0.1.5

Previous products, releases and versions have not been tested for the presence of this vulnerability because, in accordance with section 4.3.3.3 of the Software Error Correction Support Policy:

http://metalink.oracle.com/metalink/plsql/showdoc?db=Not&id=209768.1

they are no longer being patched. Customers using previous versions must update, and customers using previous releases must upgrade, to a version and release on which security patches for this vulnerability are available.

E-Business 11*i* Impact
Oracle E-Business Suite Release 11*i* customers must apply the patches listed in the "Patch Availability Matrix" to existing environments as they correspond to their current RDBMS release.

Platforms Affected
See Patch Availability section, below.

Required Conditions for Exploit
An authenticated database user (i.e., valid login required) with the ability to invoke SQL is required to exploit these vulnerabilities. SQL is part of the core component of an Oracle Database Server and Oracle users are granted access to SQL by default in Oracle Database Server.

Risk to Exposure
Risk to exposure is moderate since a malicious user must first be authenticated to the database. However, potential impact can be high as an authenticated, knowledgeable and malicious user can exploit these vulnerabilities to cause a Denial of Service (DoS) attack against and/or capture an active user session of the Oracle9*i* Database Server.

How to Minimize Risk
There is no workaround that fully addresses the security vulnerabilities described in this Alert.

Ramification for Customer

Oracle strongly recommends that customers apply the patch. Please 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 258254.1:

http://metalink.oracle.com/metalink/plsql/ml2_documents.showDocument?p_database_id=NOT&p_id=258254.1

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

Please review MetaLink, or check with Oracle Support Services periodically for patch availability if the patch for your platform is unavailable. Oracle strongly recommends that you comprehensively test the stability of your system upon application of any patch prior to deleting any original files that are replaced by the patch.

References

http://www.nextgenss.com/advisories.html

Credits

Oracle Corporation thanks David Litchfield of Next Generation Security Software Ltd., for discovering and promptly bringing this potential security vulnerability to Oracle's attention.

Modification History

18-FEB-04: Initial release, version 1

20-MAY-04: Added 9.0.1.5 and reference to Software Error Correction Support Policy.