

[VulnWatch] Integrigy Security Advisory – High Risk Security Issues in the Oracle Database and Oracle Applications

Source: <http://www.derkeiler.com/Mailing-Lists/VulnWatch/2005-01/0042.html>

From: Integrigy Security (*alerts_at_integrigy.com*)

Date: 01/20/05

To: <vulnwatch@vulnwatch.org>

Date: Wed, 19 Jan 2005 22:09:58 -0600

Integrigy Security Advisory

High Risk Security Issues in the Oracle Database and Oracle Applications

Oracle Critical Patch Update – January 2005

January 19, 2005

Summary:

Oracle has released its first Critical Patch Update (January 2005) and fixes 23 vulnerabilities in the Oracle Database, Oracle Application Server, and Oracle E-Business Suite – Integrigy discovered 5 of these vulnerabilities. The vulnerabilities in the Oracle Database and Oracle E-Business Suite should be considered high risk and organizations should work to apply the necessary patches at the earliest possible opportunity.

Integrigy Discovered Vulnerabilities:

Product: Oracle E-Business Suite

Versions: 11.0.x, 11.5.1 – 11.5.9

Platforms: All platforms

Risk Level: High

Number: 2

Product: Oracle Database

Versions: 8.1.7.x, 9.0.1.x, 9.2.0.x, and 10.1.0.x

Platforms: All platforms

Risk Level: High

Number: 1

Product: Oracle Application Server

Versions: 1.0.2.2.x

Platforms: All platforms

Risk Level: Medium

Number: 2

Description:

Oracle Corporation released the first Critical Patch Update (CPU) on January 18, 2005. The CPU is a collection of security related patches for the Oracle Database, Oracle Application Server, Oracle Collaboration Suite, and Oracle E–Business Suite. There are 23 vulnerabilities addressed in the CPU ranging from buffer overflows to SQL injection to denial of service (DoS) issues. Most of the vulnerabilities are high risk and should be addressed quickly by organizations.

Oracle Database Vulnerabilities:

Multiple vulnerabilities exist in the Oracle Spatial package MDSYS.MD2 that can be exploited by an attacker to gain escalated privileges on the server.

Oracle Application Server Vulnerabilities:

A denial of service vulnerability exists in the Oracle Forms Server.

The Oracle Reports Server administrative functions can be exploited to obtain the database password used by the server. Integriqy released a security alert in November 2002 (www.integriqy.com/alerts/ReportsServer_APPS_Disclosure.htm) to notify Oracle Applications clients of the issue and to provide a work–around. The Oracle patch removes the password from being displayed. However, Integriqy still recommends clients install the work–around in order to block access to all the administrative functions.

Oracle E–Business Suite Vulnerabilities:

Two SQL injection vulnerabilities exist in the Oracle E–Business Suite.

Solution:

All Oracle customers should consider these vulnerabilities high risk and apply the Oracle patches at the earliest possible opportunity. Customers with Internet facing application servers should consider applying these patches as soon as possible. See Oracle Metalink Note 293953.1 for patch information and instructions.

In order to assist our clients, Integriqy has developed a detailed analysis of the security release and its impact on Oracle Applications. The analysis provides additional information on the vulnerabilities and patches released in the Critical Patch Update as it relates to the Oracle E–Business Suite (Oracle Applications 11i). The objective of the analysis is to assist IT managers and Applications DBAs in assessing the impact on their Oracle Applications 11i implementations and the risks associated with the

vulnerabilities, especially since the CPU addresses a large number of vulnerabilities and impacts all layers of the Oracle Applications technology stack. The analysis can be downloaded from Integrigy's website at www.integrigy.com/info/SecurityAnalysis-CPU0105.pdf.

For more information or questions regarding this security alert, please contact us at alerts@integrigy.com.

Integrigy has included checks for many of these vulnerabilities in AppSentry, a vulnerability scanner for Oracle Applications, and AppDefend, an application intrusion prevention system for Oracle Applications.

Credit:

The vulnerabilities referenced in this advisory were discovered by Stephen Kost of Integrigy Corporation.

About Integrigy Corporation (www.integrigy.com)

Integrigy Corporation is a leader in application security for large enterprise, mission critical applications. Our application vulnerability assessment tool, AppSentry, assists companies in securing their largest and most important applications. AppDefend is an intrusion prevention system for Oracle Applications and blocks common types of attacks against application servers. Integrigy Consulting offers security assessment services for leading ERP and CRM applications.

For more information, visit www.integrigy.com.