

Flaws Show Need to Update Oracle Product Management Practices

Rich Mogull

A new set of critical vulnerabilities shows that Oracle can no longer be considered a bastion of security. Database and application managers must begin protecting and maintaining Oracle systems more aggressively.

NEWS ANALYSIS

Event

On 17 January 2006, Oracle released its latest Critical Patch Update (CPU), which includes patches for 82 vulnerabilities across multiple product lines, including: all currently supported Oracle databases; Oracle Application Server; Oracle Enterprise Manager; Oracle Collaboration Suite; Oracle E-Business Suite; PeopleSoft applications; and JD Edwards applications. Oracle has made information on related security issues and practices available at:

- www.oracle.com/technology/deploy/security/pdf/twp_security_checklist_db_database.pdf
- www.oracle.com/technology/deploy/security/pdf/cpu_whitepaper.pdf
- www.oracle.com/technology/deploy/security/pdf/cpujan2006.html

Analysis

Gartner supports the quarterly CPU program, which enables system administrators to plan and schedule Oracle maintenance. However, the range and seriousness of the vulnerabilities patched in this update cause us great concern. The database products alone include 37 vulnerabilities, many rated as easily exploitable and some potentially allowing remote database access. Oracle has not yet experienced a mass security exploit, but this does not mean that one will never occur.

Many Oracle administrators rely on a combination of the company's historically strong security and the fact that Oracle applications and databases are typically located deep within the enterprise, and so neglect to patch their systems regularly. Moreover, patching is sometimes impossible, due to ties to legacy versions that Oracle no longer supports. These practices are no longer acceptable, because:

- Critical Oracle vulnerabilities are being discovered and disclosed at an increasing rate, and exploit tools and proof-of-concept code are appearing more regularly on the Internet.
- Oracle provides only very limited information about vulnerabilities — far less than is industry-standard — making it difficult for enterprises to evaluate the risk. The company sometimes patches internally discovered vulnerabilities without releasing details.
- The quality and ease of use of Oracle patches still require improvement, because of reported installation and stability problems.
- Oracle does not describe manual "workarounds," because they typically do not work across the entire stack of Oracle products. This practice makes it difficult for managers of Oracle systems to make informed risk decisions.

Recommendations for enterprises using Oracle databases and applications

1. Move immediately to shield these systems as well as possible, using firewalls, intrusion prevention systems and other technologies. Develop a shielding schedule that coincides with Oracle CPU release dates.
2. Apply the available patches as rapidly as possible, because incomplete information from Oracle will necessarily make shielding incomplete.

3. Use alternative security tools, such as activity-monitoring technologies, to detect unusual activity.
4. Pressure Oracle to change its security management practices.

Analytical Source: Rich Mogull, Gartner Research

Recommended Reading and Related Research

- "Visibility and Control Are Key to Managing IT Security Vulnerabilities" — Vulnerability management must adapt to the visibility and control challenges of new IT service delivery methods. **By John Pescatore, Mark Nicolett and Amrit Williams**
- "Organizations Must Employ Effective Data Security Strategies" — Organizations can best protect data through a hierarchical data security approach that accounts for host, application and network security. **By Rich Mogull**

(You may need to sign in or be a Gartner client to access the documents referenced in this First Take.)

REGIONAL HEADQUARTERS

Corporate Headquarters

56 Top Gallant Road
Stamford, CT 06902-7700
U.S.A.
+1 203 964 0096

European Headquarters

Tamesis
The Glanty
Egham
Surrey, TW20 9AW
UNITED KINGDOM
+44 1784 431611

Asia/Pacific Headquarters

Gartner Australasia Pty. Ltd.
Level 9, 141 Walker Street
North Sydney
New South Wales 2060
AUSTRALIA
+61 2 9459 4600

Japan Headquarters

Gartner Japan Ltd.
Aobadai Hills, 6F
7-7, Aobadai, 4-chome
Meguro-ku, Tokyo 153-0042
JAPAN
+81 3 3481 3670

Latin America Headquarters

Gartner do Brazil
Av. das Nações Unidas, 12551
9º andar—World Trade Center
04578-903—São Paulo SP
BRAZIL
+55 11 3443 1509