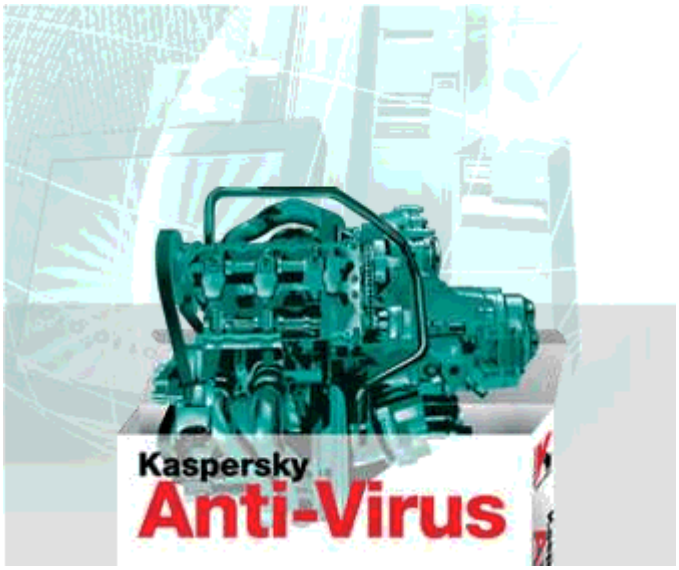
Oracle patches 36 flaws

Dan Kaplan 19 Apr 2006 21:01

Oracle released its quarterly critical patch update (CPU) Tuesday, correcting 36 flaws on company products, including its database, application server and other business applications.



Most notable among them is a fix for the PL/SQL Gateway, which acts as proxy between the web server and the database back-end server. If the existing vulnerability is exploited, a malicious hacker could take over as database administrator and gain access to the database.

British security researcher David Litchfield reported this flaw to Oracle last October and than chastised the company at this year's Black Hat Federal security conference for not fixing in its first CPU of the year. Oracle shot back, accusing Litchfield of putting its customers at risk.

Tuesday's CPU also fixed 14 database flaws, five in the Collaboration Suite and 15 in the E-Business Suite. The update included the release of an enhanced default password scanner to prevent unauthorized hacker access as well.

"Customers should apply this CPU as quickly as possible within their change-management cycle," said Ron Ben-Natan, Guardium chief technology officer, a Waltham, Mass., database security and compliance firm. "Many of the vulnerabilities are easy to exploit and do not require advanced knowledge or skills."

This update contained considerably less patching than the previous two critical updates. In January, the Redwood Shores, Calif., company issued fixes for 82 flaws and in October remedied another 80.

The impact of these vulnerabilities varies depending on the product, component, and configuration of the system. Potential consequences include the execution of arbitrary code or commands, information disclosure, and denial of service. Vulnerable components may be available to unauthenticated, remote attackers. An attacker who compromises an Oracle database may be able to gain access to sensitive information.

A Gartner analyst slammed Oracle in January, saying the size of the latest CPUs proves "Oracle can no longer be considered a bastion of security."

In November 2004, Oracle began issuing updates four times a year. At the time, company Chief Security Officer Mary Ann Davidson said quarterly releases would not leave users exposed for long but also would not overwhelm them with the need for constant fixes.

Related News Stories

IDM: Moving up
Cover story: Defining trust
Firm: Oracle released flaw info by mistake
NTT joins Liberty Alliance board
News briefs
2 minutes on...Third-party patch?

Related Links

Oracle security alerts