Oracle Patches 36 Bugs, Risk Ranked At '10'

(URL: http://www.crn.com/sections/software/software.jhtml?articleId=186100274)

By Gregg Keizer,

1:36 PM EDT 2006 ,19 .הט ו.:

Oracle Corp. on Tuesday released its quarterly patch batch, plugging 36 vulnerabilities in several of its products, including the flagship Oracle Database.

Although the number of fixes may seem high, it's actually less than half of the last Oracle bunch, which counted 82 fixes.

Oracle's Critical Patch Update (CPU) for April contains 14 patches that fix the three-dozen flaws, several of which the company said could be easily and broadly exploited. Most of the bugs could be attacked remotely.

Although Oracle doesn't use a ranking system similar to Microsoft's or Apple's that detail the most critical vulnerabilities, in a separate alert to its customers security giant Symantec rated the urgency of patching as "10," its highest ranking. Danish vulnerability tracker Secunia, meanwhile, tagged the CPU as "Highly critical," its second-from-the-top rating.

"Several of these vulnerabilities are significant, and should be patched as soon as possible," Symantec wrote to subscribers of its DeepSight Threat Management System. "No workarounds for these issues have been published by Oracle."

Ron Ben-Natan, the chief technology officer of database security company Guardium, agreed. "Many of the vulnerabilities are easy to exploit and do not require advanced knowledge or skills," he said in an e-mail to TechWeb on Wednesday.

"Identity thieves search for the weakest link in database security, often using one small vulnerability to compromise multiple subsystems within the database engine," Ben-Natan added. "These patches are essential."

Tuesday's bugs affect Oracle Database, Oracle Application Server, Oracle Collaboration Server, Oracle E-Business Suite and Applications, Oracle Pharmaceutical Applications, Oracle Enterprise Manager, and Oracle Peoplesoft Enterprise and JD Edwards EnterpriseOne.

As always, Oracle remained tight-lipped about the vulnerabilities, although it published a risk matrix in its advisory to guide system administrators in prioritizing the patch process. Among the bugs Oracle patched was one within the PLSQL (Procedural Language/Structured Query Language) Gateway, software used by several Oracle products, including Application Server and HTTP Server, to tie the company's database with Web-based apps.

Earlier this year, David Litchfield, managing director of U.K.-based Next Generation Security Software (NGS) and a frequent Oracle critic, tussled with the Redwood Shores, Calif.-based company over the PLSQL vulnerability. At the Black Hat Federal 2006 conference in late January, Litchfield disclosed the zero-day bug, called it "critical," and produced an unsanctioned fix.

At the time, Litchfield hammered Oracle for slow patching. "I don't think leaving their customers vulnerable for another 3 months (or perhaps even longer) until the next CPU [Critical Patch Update] is reasonable," he said then, "especially when this bug is so easy to fix and easy to workaround."

Tuesday, however, Oracle's advisory credited Litchfield, among several others, as having brought bugs to its attention.

Also on Tuesday, Litchfield said in an entry to the Full Disclosure security mailing list that NGS would withhold details of the numerous new Oracle bugs it had uncovered.

"Full details will be published on the Tuesday, 18th of July 2006. This three month window will allow Oracle database administrators the time needed to test and apply the patch set before the details are released to the general public," he said.

Patches for the 36 vulnerabilities can be downloaded by Oracle users from the Metalink site.
