

MySQL corregge gravi falle

05/05/06

Il noto database open source più utilizzato nella rete è stato aggiornato, in quanto nei giorni scorsi sono stati scovate diverse vulnerabilità tra cui una grave. Le falle scovate nel famoso MySQL sono tre, due di queste riguardano sempre lo stesso file cioè: sql_parse.cc e l'ultima, la più pericolosa, si riferisce al file: sql_base.cc. La vulnerabilità più grave permette ad un attacker di sfruttare da remoto un Buffer Overflow () ed eseguire codice arbitrario. Il problema si verifica quando viene inviato un pacchetto malformato a "COM_TABLE_DUMP", questo genera il problema prima citato. Gli altri due bug invece sono di minore importanza, anche se non da sottovalutare in quanto danno la possibilità (da remoto) di accedere ad alcune porzioni di memoria. MySQL AB, la società svedese creatrice dell'omonimo database open source ha già rilasciato le patch di aggiornamento che coprono queste vulnerabilità. Si consiglia l'immediata applicazione in quanto in rete sono già disponibili gli exploit per sfruttare tali falle.

fonte: www.orebla.it

link: http://www.orebla.it/module.php?n=news_050506_2