Attenzione: vulnerabilità Joomla versioni 1.5.x

di Paolo Franzese

Nei giorni scorsi il Supporto Ufficiale al noto Cms Joomla ha annunciato la scoperta di una falla di sicurezza presente in tutte le versioni 1.5.x. Tale vulnerabilità consente ad un malintenzionato di editare la Password dell'account Amministratore sfruttando la funzionalità di ripristino password messa a disposizione dal componente "com_user". Se sfruttata, infatti, tale vulnerabilità consente di accedere come Amministratori al Pannello Admin di Joomla e, tramite questo, permette di editare pagine (defacing), leggere i contenuti dei file, modificare i dati del Database, etc. In particolare una volta eseguita tale modifica alla password è possibile visionare il contenuto del file "configuration.php" e, di conseguenza, impossessarsi dei dati Ftp e MySQL che sono riportati in chiaro nello stesso file.
Descrizione della Vulnerabilità e relativa FIX:
http://developer.joomla.org/security/news/241-20080801-core-password-remind-functionality.html
http://www.joomlaitalia.com/content/view/323/90/

Da un articolo scritto da Paolo Franzese il 15 Settembre 2008

Contatti +39 388 1020417 - info@imaginepaolo.com