Portuguese software detects flaws on 5 opensource programs

Security flaws that may allow illegitimate access to databases or remote control by a third party to a browser in use, are some of the main vulnerabilities reported by the Portuguese company Dognædis, that disclosed today the results of an analysis to opensource software.

Of the 25 programs analyzed, five contained "bad", "very bad" or "critical" security flaws, in a total of 31 vulnerabilities, unknown until this date, detected by CodeV – a security solution, launched in September, that analyzes the source code of web applications in order to detect security flaws.

The results of the vulnerability tests to software "used by thousands of people worldwide" revealed fragility on the webmail clients Hastymail and Atmail – very used by security forces and north-american universities – and on solutions such as ZenCart (a framework to embed shopping carts on websites), PrestaShop and osCommerce.

Of the referred lot, the programs more used by Portuguese companies shall be Prestashop and osCommerce, open source solutions of online store that have also a great popularity as a worldly basis, explained to TeK Francisco Rente, researcher of the University of Coimbra and executive director of Dognædis.

Another popular solution tested by CodeV was SugarCRM, on which there was not found any vulnerability, exemplified the responsible. He noted however that the analysis was carried strictly over the open part of the code, that is usually complemented with add-ons.

Concerning the vulnerabilities found, there were saliented, by instance, the possibility of

being carried SQL injection attacks, to illegitimate database access or XSS, that may allow third party control of the browser of the user with a flawed application. This latter affects both webmail clients (Hastymail and Atmail) where it was also detected a critical flaw that allows the injection of malicious code.

The flaws now presented are added to the 28 found on the "40 largest free software existent on the market", disclosed with the CodeV launch. The new results have been previously shared with the projects responsible and are available to a detailed consult at Dognædis' website.

Translation from the original.