CPG Dragonfly CMS *meta* and URL Cross-Site Scripting Vulnerabilities

2012-02-21 13:52:15 by Raven

SECUNIA ADVISORY ID: SA47999

VERIFY ADVISORY: Secunia.com http://secunia.com/advisories/47999/

RELEASE DATE: 2012-02-21

DESCRIPTION: Ariko-Security has discovered two vulnerabilities in CPG Dragonfly CMS, which can be exploited by malicious people to conduct cross-site scripting attacks. The vulnerabilities are confirmed in version 9.3.3.0. Other versions may also be affected. 1) Input passed via the "meta" parameter to index.php (when "name" is set to "coppermine" and "file" is set to "thumbnails") is not properly sanitised before being returned to the user. This can be exploited to execute arbitrary HTML and script code in a user's browser session in context of an affected site. This vulnerability may be related to: SA18940
2) Input passed via the URL to index.php (when "name" is set to "coppermine") is not properly sanitised before being returned to the user. This can be exploited to execute arbitrary HTML and script code in a user's browser session in context of an affected site. Successful exploitation of this vulnerability requires "Enable debug mode" of the coppermine configuration to be enabled (enabled by default).

SOLUTION: Edit the source code to ensure that input is properly sanitised. Disable "Enable debug mode" within the coppermine configuration.
PROVIDED AND/OR DISCOVERED BY: Ariko-Security
ORIGINAL ADVISORY: Ariko-Security: http://advisories.ariko-security.com/2012/audyt_bezpieczenstwa_1m2.html