Referaat: CVE-2014-2664

X2Engine CRM system compromise

Tudeng: Anton Prokopov

Õppejõud: Meelis Roos

Tartu 2014
What is X2CRM system?

It's small business marketing automation and sales force customer relationship management system, as they say on their web-page.

X2Engine is a next-generation, open source social sales application for small and medium sized businesses. It was designed to streamline contact and sales actions into one compact blog-style user interface. Add to this contact and colleague social feeds and sales representatives become smarter and more effective resulting in increased sales and higher customer satisfaction.

That's how X2Engine looks like

You can see the live demo of the X2Engine on their web-page or just by clicking here: watch demo.

Vulnerability

System seems to be complicated and considered, but it still has vulnerabilities. I'm talking now about one Secunia team found out. Problem was found in protected/controllers/ProfileController.php script, which has "ProfileController::actionUploadPhoto" method. This method allows uploading of files with arbitrary extensions to a folder inside the webroot. Due to this method anyone can upload a malicious PHP script file to the server and then execute arbitrary PHP code. It might cause real troubles, because with that kind of script it's possible not only to broke the program and cause some problems with user business, but to steal important information about the business management or even clients.
Solution

By now X2Engine has released a vendor patch that fixes this vulnerability and two more versions of the program itself that already include this patch by default. (Starting from version 4.0).

It's not enough to say "All you need to fix this vulnerability is to install the patch", so I found out, what fixes were implemented generally.

The arbitrary file type upload vulnerability is fixed now: there will be a site-wide action filter that halts the action if the filename or mime-type are within lists of blacklisted extensions or types, so nobody can upload executable files. It's important to close XSS attack vectors (unfiltered output) as well and it's already done, at least the larger part. One of the developers is doing an audit of the codebase to find all potential sources of SQL injection, and this will cover the aforementioned vulnerability. He's already fixed numerous instances of it and successfully keeps doing.

Is that enough?

The problem was in executing malicious PHP scripts on the server by uploading them using "ProfileController::actionUploadPhoto" method. The solution is sufficient, because it allows no uploading files with extensions that are in the blacklist. There is no way now to upload script to the server and then execute it. Also developers found some more vulnerabilities, for example SQL injections and already fixed them, so it's possible to say, that solution is even more that just sufficient.

Resources:


http://x2community.com/topic/1511-multiple-vulnerabilities-in-x2engine/#entry7354