Umbraco CMS TemplateService Remote Code Execution Vulnerability

29/11/2013

Software:	Umbraco CMS
Affected Versions:	Umbraco CMS versions prior to 6.0.4
CVE Reference:	CVE-2013-4793
Author:	MWR Labs (http://labs.mwrinfosecurity.com/)
Severity:	High
Vendor:	Umbraco
Vendor Response:	Fix Released

Description:

MWR Labs have discovered a vulnerability in Umbraco CMS, which would allow an unauthenticated attacker to execute arbitrary ASP.NET code on the affected server.

The vulnerability exists in the TemplateService component, which is exposed by default via a SOAP-based web service.

Impact:

By exploiting this vulnerability, an attacker would be able to update the contents of any template. MWR have developed a proof of concept exploit which updates the default site template to contain an ASP.NET shell. Subsequent requests to any page using this template will execute this code on the compromised server.

Cause:

The vulnerability is caused due to the update() function not checking that the user has authenticated before processing the request. The functionality of update() allows a user to update the contents of templates for the CMS. This vulnerability can be exploited by sending a specially crafted SOAP request to the TemplateService component, updating the CMS template to contain malicious ASP.Net code.

It should be noted that this vulnerability affects instances of Umbraco CMS, even when the web services interface is not explicitly enabled.

Interim Workaround:

The vendor recommends deleting umbraco.webservices.dll, which is the library responsible for processing web services requests.

Solution:

The vendor has released a fix for this issue, which removes the web services component completely.

If it is not possible to apply this fix, MWR propose adding a call to the Authenticate() function at the start of the TemplateService update() function. It should be noted that this is not an approved fix by the vendor, and care should be taken to ensure that this does not affect the operation of the application.

Technical details

The vulnerable code from the TemplateService class (src/umbraco.webservices/templates/templateService.cs) is shown below:

```
[WebMethod]
public void update(templateCarrier carrier, string username, string password)
    ...
    cms.businesslogic.template.Template template;
    try
    {
        template = new cms.businesslogic.template.Template(carrier.Id);
    }
    ...
    template.Design = carrier.Design;
    template.Save();
```

The update() function takes an attacker-controlled carrier structure, as well as the username and password provided to authenticate to the web service. Unlike most of the other web methods, the update() function ignores the username and password values, and does not authenticate the request.

The function goes on to retrieve an existing template by its Id, which is specified in the carrier value. After selecting a valid template, it updates the contents of the template using the carrier's "Design" field. It then saves the content to the database for use in future requests.

Detailed Timeline

Date:	Summary:
04/03/2013	Vendor contacted, request for a PGP key
08/04/2013	Initial vulnerability details disclosed
17/04/2013	Vendor indicates a patch has been developed. No immediate release as vendor believes this would not be exploitable in the default configuration
26/04/2013	After discussion, vendor realises the issue affects all deployments. Version 6.0.4 released that fixes the issue
17/05/2013	Vendor requests a delayed release of this advisory to allow customers to update
28/11/2013	Advisory released