

microsoft.public.inetserver.iis.security: Re: IIS Extensions in URL causes filter to break.

Re: IIS Extensions in URL causes filter to break.

Source: <http://www.derkeiler.com/Newsgroups/microsoft.public.inetserver.iis.security/2003-06/1179.html>

From: David Wang [Msft] (*someone_at_online.microsoft.com*)

Date: 06/27/03

Date: Thu, 26 Jun 2003 19:14:19 -0700

I installed Q811114 on W2KSP3 to verify. I see SF_NOTIFY_URL_MAP fired at least once for all three of the IMG source URLs. In fact, I see it fire twice for every such URL that is scriptmapped (and only once for URL that is not scriptmapped), both before and after Q811114.

The difference between the two is the content of pszUrl and pszPhysicalPath on the first event firing of every URL.

1st Event Firing. Suppose the request is for

<http://www.myserver.com/host.asp/mystring/mylogfile1>

pszUrl = /Host.asp

pszPhysicalPath = C:\inetpub\wwwroot\Host.asp

2nd Event Firing

pszUrl = /Host.asp/mystring/mylogfile1

pszPhysicalPath = C:\inetpub\wwwroot\Host.asp\mystring\mylogfile1

Before Q811114, both events had the same pszUrl and pszPhysicalPath value as the 2nd Event Firing. I suspect that your filter has some dependency on the values in the first firing of SF_NOTIFY_URL_MAP.

If your filter operates the way you say, this shouldn't bother it; you'd ignore the first fired event, and on the second firing of the event, you'll find your trigger in the URL and do your custom action. The fact that the intermediate values of SF_NOTIFY_URL_MAP may change happens to be completely arbitrary behavior; IIS can only say that one or more of the events contain actually correct data but not tell you which (correctness depends on what other ISAPI actions are, and since you're seeing things as it happens, data values can truly be in flux). SF_NOTIFY_URL_MAP event happens when a URL-to-PhysicalPath mapping happens in IIS, and it happens at least once for every request, and maybe more than once, depending on whether the URL causes IIS to request any more URL-to-PhysicalPath mappings. Certain ServerVariables trigger this. Certain codepaths involving the Scriptmapped code path (vs static file handler) also trigger this.

As for the order of handling between ISAPI Extensions and Filters – Filters that register for request-side events (ReadRawData, PreprocHeaders, UrlMap, Authentication, AuthComplete, AccessDenied) trigger prior to any Extensions

Re: IIS Extensions in URL causes filter to break.

microsoft.public.inetserver.iis.security: Re: IIS Extensions in URL causes filter to break.

being invoked. SendResponse and SendRawData events will intermingle with HttpExtensionProc actions (for example, HSE_REQ_SEND_RESPONSE_HEADER_EX trigger SendResponse and SendRawData events, and WriteClient triggers SendRawData event, etc). Finally, Log, EndOfRequest, and EndOfNetSession happen after IIS has "processed" the request.

Now, I wonder if your filter can use SF_NOTIFY_PREPROC_HEADER instead of SF_NOTIFY_URL_MAP. You can get the URL and send a response in SF_NOTIFY_PREPROC_HEADER as well, and you don't have the baggage of SF_NOTIFY_URL_MAP.

```
--
//David
This posting is provided "AS IS" with no warranties, and confers no rights.
//
"Abh Khush" <montul7@yahoo.com> wrote in message
news:578a2046.0306260738.53bceb67@posting.google.com...
Here are some clarifications
1) I delete all cached files at the browser to ensure that the browser
follows the url of <img> to IIS
2) It has nothing to do with .asp per se - it can be any registered
extension. Try with any entry from MetaBase under
[LM/W3SVC]
".id=6014;Name=ScriptMaps;Data=.ida,C:\WINNT\System32\idq.dll,3,GET,HEAD,POS
T
.idq,C:\WINNT\System32\idq.dll,3,GET,HEAD,POST
.asp,C:\WINNT\System32\inetsrv\asp.dll,1,GET,HEAD,POST,TRACE"
(actually, I first noticed the problem with my own registered
extension.)
3) The static page which has the <img> URLs always exists.
4) In the <img> SRC URL /host.asp does not exist.
5) I confirmed using NetMon on IIS server that the static HTML is
requested always followed by one request for each <img> URLs in it
irrespective of how the <img> urls look. (after the browser cache is
cleared)
6) This happens only with the Q811114 patch, not prior to that. If you
remove the patch, things work again.
Given the above conditions, the <IMG> url does not fire OnUrlMap
"atleast once" as you point. Some URLs are requested more than once,
some others are not requested at all. The behavior is not consistent
each time.
What my filter does exactly?
It filters every incoming request looking for "mystring" inside it.
e.g 
If it finds "mystring" then it extracts the image id "myimageid",
finds the corresponding file name for this image id from an image
id/filename table inside my filter, reads the file from disk, and
finally writes the file to the client through the HTTPFilterContext
object.
If it does not find "mystring" it does nothing.
Because of this all my images on the rendered static page are
scrambled or "not found". Image links meant for image1 display image2
etc.
I also tested with another dummy filter that does not do any
processing of the URLs, and I can see the same problem when I step
through OnUrlMap.
Note that, if you remove the registered extension from the <img> URLs,
OnUrlMap gets fired once for every URL in the static HTML. (after the
browser cache is cleared)
```

Re: IIS Extensions in URL causes filter to break.

microsoft.public.inetserver.iis.security: Re: IIS Extensions in URL causes filter to break.

What are your thoughts? Also, can you explain what is the order in which IIS handles extensions and filters. My understanding is that any request first goes through all registered filters and then to the registered extensions.

Thanks for your time,

Abhinav

"David Wang [Msft]" <someone@online.microsoft.com> wrote in message news:<ehk6iQ7ODHA.3020@TK2MSFTNGP10.phx.gbl>...

> Can you clarify what you are saying in step #3. I'll first offer a few
> thoughts on the matter.

>

> First, IIS does NOT "request" the URL of the in an HTML file. When
> you browse the HTML file, the browser first reads the HTML file, and at
> its

> discretion, it may retrieve the URL of its contents (i.e. follow the URL
> of

>). For example, caching at the browser affects this behavior.

>

> Second, OnUrlMap is only guaranteed to fire at least once per retrieval of
> a

> URL. It can fire more than once for each URL, and it can contain
> different

> values on each firing. Certainly, if a URL isn't fetched for an HTML page
> for whatever reason, it's not going to fire, either.

>

> Finally, in the SRC URL, does /host.asp exist?

>

> For example, if an ASP page retrieve PATH_TRANSLATED and certain other
> server variables, it will trigger a SF_NOTIFY_URL_MAP on its own. On the
> other hand, a plain static file request likely ends up only triggering
> SF_NOTIFY_URL_MAP once (unless it's invoking a DefaultDoc...).

>

>

> Please help me understand what exactly you are trying to do with your
> ISAPI

> Filter and how you are doing it, exactly. Based on what you said in step
> #3, I haven't seen anything "out of the ordinary".

>

> --

> //David

> This posting is provided "AS IS" with no warranties, and confers no
> rights.

> //

> "Abh Khush" <montul7@yahoo.com> wrote in message

> news:578a2046.0306230627.feaad22@posting.google.com...

> Hi

>

> On IIS 5.0/5.1, after applying the security hotfix Q811114, I have
> started to see the following problem.

>

> Steps to reproduce

> 1) Create an IIS HTTP filter and override OnUrlMap. (e.g let's filter
> 'mystring')

>

> 2) Create an HTML page with few img links in it containing a
> registered extension and which has to be parsed by the filter.

>

> Here's how the html should look like.

>

> <html>

> <head><title>Some static page</title></head>

> <body>

microsoft.public.inetserver.iis.security: Re: IIS Extensions in URL causes filter to break.

```
> <img
> src="http://www.myserver.com/something/host.asp/mystring/mylogfile1">
> <img
> src="http://www.myserver.com/something/host.asp/mystring/mylogfile2">
> <img
> src="http://www.myserver.com/something/host.asp/mystring/mylogfile3">
> </body>
> </html>
>
> 3) When you hit the static page containing the above links and step
> into the OnUrlMap function inside your filter, you will see that the
> requests sent down to the OnUrlMap are incorrect. Instead of sending
> GET requests for these 3 urls one after the other, IIS will randomly
> request 2-3 times of one of these urls, omit some urls etc.
> If however you remove the .asp from the above urls it works fine.
>
> It is hard to convince myself that this is tightened security because
> from my understanding, IIS filters are always called before any IIS
> extensions are. And if that is the case then the GET requests should
> be sent down correctly into OnUrlMap.
>
> Can some one on the MS IIS team please explain?
>
> Thanks,
> Abhinav
```