IIS解析漏洞

IIS7.X解析漏洞

漏洞介绍

1、IIS7.x在解析ASP文件的时候不存在解析漏洞，

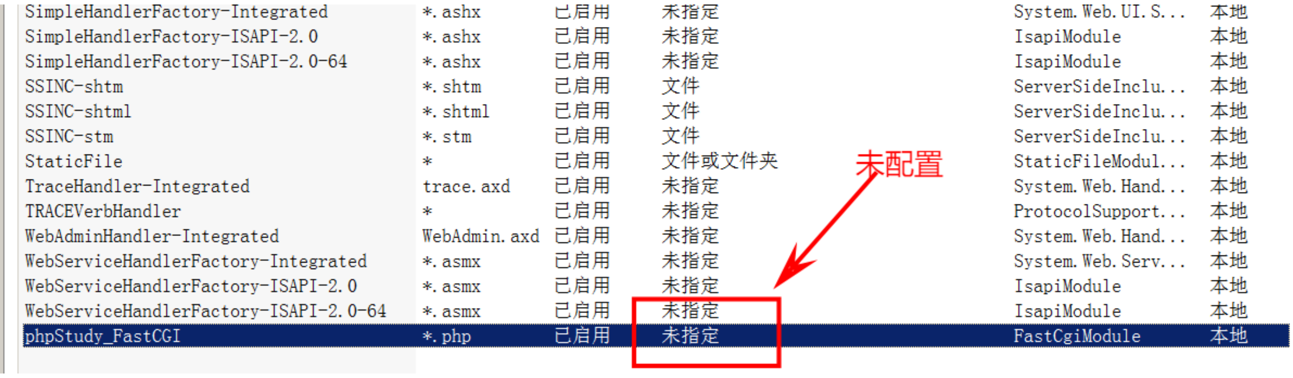
2、解析PHP文件时，如果PHP配置文件cgi.fix_pathinfo=1，那么就有解析漏洞，如：`http://www.xxx.com/x.jpg/x.php`的时候，如果x.php不存在，php就会向前解析，如果x.jpg存在，会把x.jpg当作php文件解析，这样就产生了漏洞

漏洞原理

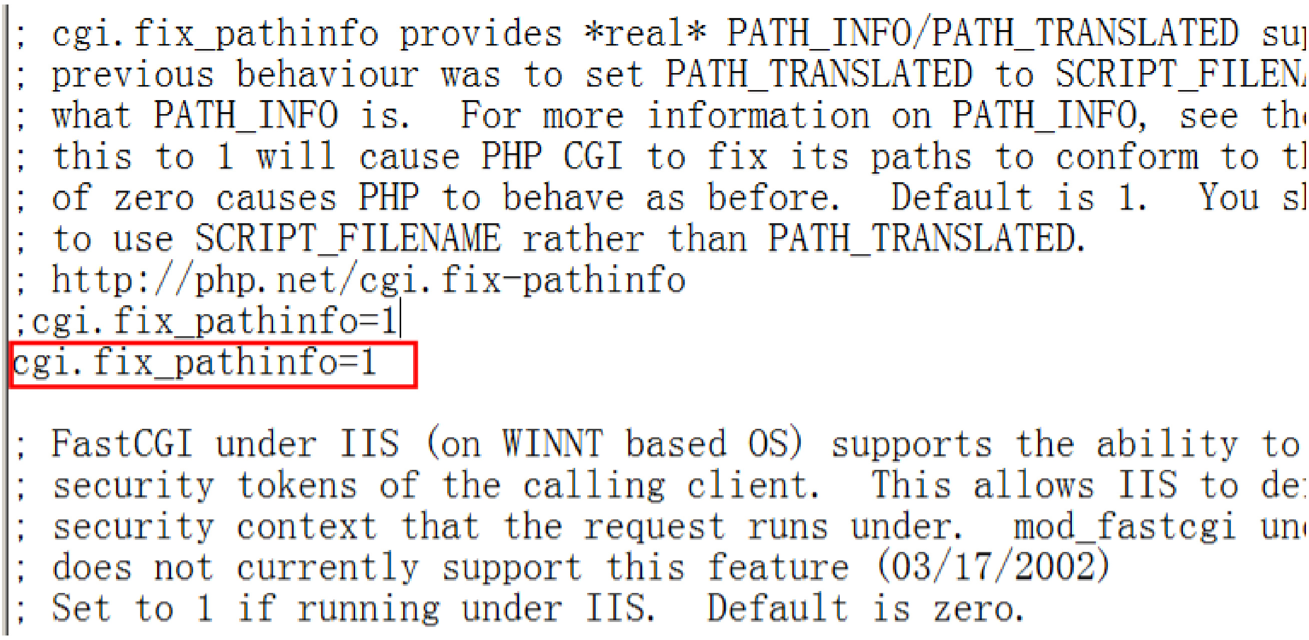
1、存在条件

`(1)在IIS7.x中配置了处理程序映射中的FastCGI,并且【路径类型】未配置`

`(2)PHP中的PHP.INI文件配置了cgi.fix_pathinfo=1`



SimpleHandlerFactory-Integrated	*.ashx	已启用	未指定	System.Web.UI.S...	本地
SimpleHandlerFactory-ISAPI-2.0	*.ashx	已启用	未指定	IsapiModule	本地
SimpleHandlerFactory-ISAPI-2.0-64	*.ashx	已启用	未指定	IsapiModule	本地
SSINC-shtm	*.shtm	已启用	文件	ServerSideInclu...	本地
SSINC-shtml	*.shtml	已启用	文件	ServerSideInclu...	本地
SSINC-stm	*.stm	已启用	文件	ServerSideInclu...	本地
StaticFile	*	已启用	文件或文件夹	StaticFileModul...	本地
TraceHandler-Integrated	trace.axd	已启用	未指定	System.Web.Hand...	本地
TRACEVerbHandler	*	已启用	未指定	ProtocolSupport...	本地
WebAdminHandler-Integrated	WebAdmin.axd	已启用	未指定	System.Web.Hand...	本地
WebServiceHandlerFactory-Integrated	*.asmx	已启用	未指定	System.Web.Serv...	本地
WebServiceHandlerFactory-ISAPI-2.0	*.asmx	已启用	未指定	IsapiModule	本地
WebServiceHandlerFactory-ISAPI-2.0-64	*.asmx	已启用	未指定	IsapiModule	本地
phpStudy_FastCGI	*.php	已启用	未指定	FastCgiModule	本地



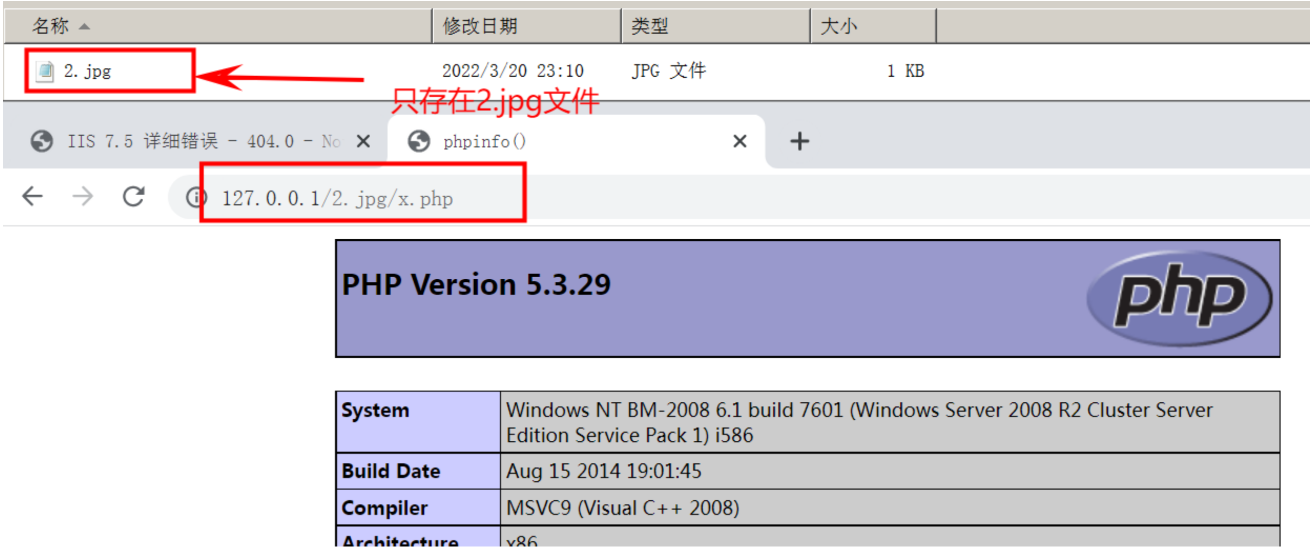
```
; cgi.fix_pathinfo provides *real* PATH_INFO/PATH_TRANSLATED su
; previous behaviour was to set PATH_TRANSLATED to SCRIPT_FILEN
; what PATH_INFO is.  For more information on PATH_INFO, see th
; this to 1 will cause PHP CGI to fix its paths to conform to t
; of zero causes PHP to behave as before.  Default is 1.  You s
; to use SCRIPT_FILENAME rather than PATH_TRANSLATED.
; http://php.net/cgi.fix-pathinfo
;cgi.fix_pathinfo=1
cgi.fix_pathinfo=1

; FastCGI under IIS (on WINNT based OS) supports the ability to
; security tokens of the calling client.  This allows IIS to de
; security context that the request runs under.  mod_fastcgi un
; does not currently support this feature (03/17/2002)
; Set to 1 if running under IIS.  Default is zero.
```

详细原理查看【CGI解析漏洞】

漏洞复现

1、当存在2.jpg，但是x.php不不存在的时候，访问`http://127.0.0.1/2.jpg/x.php`这个时候2.jpg会被当作php文件去解析



名称	修改日期	类型	大小
2. jpg	2022/3/20 23:10	JPG 文件	1 KB

只存在2.jpg文件

127. 0. 0. 1/2. jpg/x. php

PHP Version 5.3.29

System	Windows NT BM-2008 6.1 build 7601 (Windows Server 2008 R2 Cluster Server Edition Service Pack 1) i586
Build Date	Aug 15 2014 19:01:45
Compiler	MSVC9 (Visual C++ 2008)
Architecture	x86

漏洞修复

1、设置cgi.fix_pathinfo=0

2、设置处理程序映射中的FastCGI,并且【路径类型】为文件或【文件夹】