The state of MikroTik security. An overview.

Name: Kirils Solovjovs
Company: Possible Security
Position: Lead Researcher

http://kirils.org/
twitter.com/KirilsSolovjovs
hackitua@kirils.org
Outline

- RouterOS intro
- Jailbreaking
- Current vulnerabilities
- How attackers abuse this
- Current and future changes
- Surprise
Legal disclaimer

Content of this presentation may only be used by the members of the research community to aid them in assessing security and by the users to aid them in achieving interoperability of computer programs.
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
```

```
[  l i n u x - 3 . 3 . 5 . t a r _ b z 2
  l i n u x - 3 . 3 . 5 . t a r _ q g
  l i n u x - 3 . 3 . 5 . t a r _ s i g n
  l i n u x - 3 . 3 . 5 . t a r _ x z
  l i n u x - 3 . 1 . 6 . t a r _ b z 2
  0 7 - M a y - 2 0 1 2  1 6 : 1 5
  0 7 - M a y - 2 0 1 2  1 6 : 1 5
  0 7 - M a y - 2 0 1 2  1 6 : 1 5
  0 7 - M a y - 2 0 1 2  1 6 : 1 5
  1 2 - M a y - 2 0 1 2  1 7 : 2 3
```
Closed source and closed ecosystem
Ecosystem. Possible entry points.
Jailbreaking history

- 1999 MikroTik™ v2.0 Router Software released
- 2005 2.9.8 option package & /nova/etc/devel-login introduced
- 2009 3.22 NPK signing added
- 2009 3.30 first jailbreak hints published (that I could find) - http://bbs.routerclub.com/thread-67904-1-1.html
- 2017 `mikrotik-tools` published
- 2017 5.x - 6.40.x first fully automated jailbreak tool
- 2017 6.41rc61 devel-login removed; only /pckg/option/ remains
- 2018 malwaaaaaaaaaaaaaare is trying to kill us all
Vulnerabilities

- 283i4jfkai3389
- chimay_red
- devel-login based jailbreaks
- CVE-2018-7445 samba
- CVE-2018-14847 winbox
- CVE-2018-115\{6,7,8,9\}
key = md5(username + "283i4jfkai3389")
password = user["password"] xor key
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
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)
CVE-2018-7445 samba

- Unauthenticated RCE
- Via long NetBIOS names in NetBIOS session request messages
- /nova/bin/smb SmbRmDir()
- Fixed in 6.41.3 & 6.40.7
CVE-2018-14847 winbox

- Unauthenticated predefined function execution (file read)
- Via abusing DLL download functionality
- /nova/bin/mproxy
- Fixed in 6.42.1 & 6.40.8
CVE-2018-14847 winbox
CVE-2018-1156 licupgr

- Authenticated RCE
- Via buffer overflow in sprintf()
- /nova/bin/licupgr busy_cde()
- Fixed in 6.42.7 & 6.40.9
Attackers don`t sleep
What versions are in use?

- major version
- 6 - 83.9%
- 5 - 13.9%
- 4 - 1.0%
- 3 - 0.8%
- 2 - 0.4%
What versions are in use?

<table>
<thead>
<tr>
<th>Version</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>ok</td>
<td>6.42.7 - 8.1 %</td>
</tr>
<tr>
<td>licupgr</td>
<td>6.42.6 - 8.0 %</td>
</tr>
<tr>
<td>YOLO</td>
<td>5.26 - 4.8 %</td>
</tr>
<tr>
<td>licupgr</td>
<td>6.42.3 - 3.7 %</td>
</tr>
<tr>
<td>!chimay_red</td>
<td>6.39.2 - 3.6 %</td>
</tr>
<tr>
<td>ok</td>
<td>6.43.2 - 3.2 %</td>
</tr>
<tr>
<td>!chimay_red</td>
<td>6.40.8 - 3.2 %</td>
</tr>
<tr>
<td>licupgr</td>
<td>6.42.1 - 3.0 %</td>
</tr>
<tr>
<td>ok</td>
<td>6.43 - 2.6 %</td>
</tr>
<tr>
<td>all</td>
<td>6.35.4 - 2.5 %</td>
</tr>
<tr>
<td>YOLO</td>
<td>5.25 - 2.2 %</td>
</tr>
<tr>
<td>winbox+licupgr</td>
<td>6.41.3 - 2.1 %</td>
</tr>
<tr>
<td>licupgr</td>
<td>6.42.5 - 1.9 %</td>
</tr>
<tr>
<td>all</td>
<td>6.30.4 - 1.8 %</td>
</tr>
<tr>
<td>(other)</td>
<td>49.3 %</td>
</tr>
</tbody>
</table>
Vulnerable devices

- Chimay red (www)
  - Vulnerable: 92,077
  - Not vulnerable: 174,639

- Devel-login
  - Vulnerable: 144,857
  - Not vulnerable: 121,859

- SMB
  - Vulnerable: 135,453
  - Not vulnerable: 131,263

- Winbox
  - Vulnerable: 158,151
  - Not vulnerable: 108,565

- Licugpr+www
  - Vulnerable: 215,478
  - Not vulnerable: 51,238
How are criminals abusing this

- «Thousands of MikroTik Routers Hacked to Eavesdrop On Network Traffic»
- TZSP to sniff
- Socks4 → Coinhive miner
- Scheduler to update config and restore control
How are criminals abusing this

```
[ MikroTik ] > /system scheduler print detail
Flags: X - disabled
0  name="schedule3" start-time=startup interval=30s on-event=script:□ owner="" policy=ftp,reboot,read,write,policy,test,password,sensitive run-count=22160 next-run=16:40:43
```
Recent and future changes to RouterOS
They don't want us here (6.41)

- nv::hasOptionPackage() === nv::hasPackage("option")
- has been around forever, but /nova/bin/login used devel-login
- Misguided attempt to fight users

→ mkdir /pckg/option
They really don`t want us here (6.42)

- New requirements for nv::hasPackage():
  - is not symlink
  - is stored on squashfs filesystem

→ mount -o bind /boot/ /pckg/option
Hardening (6.43)

!) api - changed authentication process;

!) btest - requires at least v6.43 Bandwidth Test client when connecting to v6.43 or later version server except when authentication is not required;

!) radius - use MS-CHAPv2 for "login" service authentication;

!) romon - require at least v6.43 RoMON agent when connecting to v6.43 or later RoMON client device;

!) webfig - improved authentication process;

!) winbox - improved authentication process excluding man-in-the-middle possibility;

!) winbox - minimal required version is v3.15;
Hardening (6.43)

- Password «fixed» as well. Uses SHA256 & ECC

```python
$.decode_user.py

{ 'comment': '', 'username': 'testing', 'group': 3, 'groupname': 'full', 'allowed_addresses': [ ], '_r20': [160, 132, 113, 230, 251, 211, 67, 192, 113, 57, 187, 178, 198, 147, 116, 90], 'password_set': True, 'allowed_ip4': '0.0.0.0', 'disabled': 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, 'permissions': '7ffe'}

{ 'comment': 'system default user', 'username': 'admin', 'group': 3, 'groupname': 'full', 'allowed_addresses': [ ], '_r20': [128, 6, 117, 72, 207, 239, 92, 218, 59, 35, 32, 42, 244, 12, 127, 170], 'password_set': False, 'allowed_ip4': '0.0.0.0', 'disabled': False, 'allowed_net4': '0.0.0.0', 'last_login': '2018 04 27 23:22:18', 'record_id': 1, 'key': '48 bf de 06 49 5a 0e 2d 09 d5 fb 27 b1 44 ec 93', 'password': '', 'index_id': 1, 'permissions': '7ffe'}
```
Update channel changes (6.44)

(FUTURE)

- bugfix → long-term
- current → stable
- rc → testing
  - contains beta and rc
- "/system backup cloud" for backup storing in cloud
jailbreak

https://github.com/0ki/mikrotik-tools
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 (6.43.2 and beyond)
What to expect in 2019?

● More malware
● More vulnerabilities
● Higher security jails
Conclusions

- Attackers are quick to adopt breaking IT security research
- Users host relatively newer versions than 1 year ago
- Upgrades are free and compatible with all hardware
  - Upgrade!!!
References

- https://n0p.me/winbox-bug-dissection/
- https://github.com/reivhax/Chimay-Red-tiny
- https://github.com/BasuCert/WinboxPoC
Jailbreak available NOW at https://github.com/0ki/mikrotik-tools