ABOUT REVIEW OF SECURITY OF ROUTEROS

May 8, 2018 MUM Japan 2018

Horigome Yoshihito

AGENDA

- Who arh you?
- In the beginning
- Threat
- Security settings
- for your reference

WHO ARE YOU?

- Horigome Yoshihito (堀米 義仁)
- @RBUG_JP の中の人
- https://www.rb-ug.jp/
- Network beginner
- 普段はHPC(high-performance computing)関連業務に従事
- 2015年のMUM Japanにも参加

初めに / In the beginning

IN THE BEGINNING

- 日本での知名度はまだまだ高くなく、使用者も多くはない。
- しかし世界規模でみるとMikrotik製品は世界中で販売されているため、多くのハッカーに狙われている
- WikiLeaksで掲載されたVault 7などもあって、脆弱性を狙った攻撃が増えている
- RouterOSのアップデートが行われていない(放置されている？)機器が、インターネットに接続された形で多くみられる
- 古いバージョンのRouterOSには脆弱性が見つかっており、運用するのには望ましい状態ではない

RouterOSが晒される脅威 / Threat

ROUTEROSが晒される脅威1

- 2017年3月、WikiLeaksがCIAの極秘作戦に関する機密文書「Vault 7」を公開
- トロイの木馬、ウイルス、マルウェアなど1000を超える独自のハッキングツールを駆使
- Windows、Mac OS、Linux、Android、iOS、IoT、自動運転技術、などありとあらゆるものに対してハッキングを行っていたとされる

CHIMEYRED

- ChimayRed – Reverse engineering of Mikrotik exploits from Vault 7 CIA Leaks. – Security List Networ
  http://seclist.us/chimayred-reverse-engineering-of-mikrotik-exploits-from-vault-7-cia-leaks.html
- BigNerd95/Chimay-Red: Working POC of Mikrotik exploit from Vault 7 CIA Leaks
  https://github.com/BigNerd95/Chimay-Red
- RouterOS 6.38.4までに存在した脆弱性を利用して、スクリプトをアップロードしたり、システムそのものを乗っ取ることができた
- RouterOS 6.38.5で対応

SLINGSHOT

- The Slingshot APT FAQ – Securelist https://securelist.com/apt-slingshot/84312/
- 先述したChimeyRedに関連しているといわれている
- 既に開発が終了しているRouterOS 5.xで使用されていたWinbox 2.x(現行は3.x)を経由して、悪意のあるdllファイルをユーザーにダウンロードさせるというもの
- 少なくとも、当時公開されていたRouterOS 6.xを適用していれば、この脆弱性に対して影響は受けない

HAJIME BOT

- IIJ Security Diary: Hajime ボットによる 8291/tcp へのスキャン活動 https://sect.iij.ad.jp/d/2018/03/293998.html
- Hajime Botnet Makes a Comeback With Massive Scan for MikroTik Routers https://www.bleepingcomputer.com/news/security/hajime-botnet-makes-a-comeback-with-massive-scan-for-mikrotik-routers/
- Vault 7関連のChimeyRedで指摘されていた脆弱性を利用したもの
- Winboxが利用する8291/tcpがOpenしているか確認し、解放されているようであればそこから感染を試みる
- RouterOS 6.41.3で対応

EXPLOIT DATABASEに掲載される脆弱性

Date ▾	D	A	V	Title	Platform	Author
2018-04-13	⬇	-	⏱	MikroTik 6.41.4 - FTP daemon Denial of Service PoC	Linux	FarazPajohan
2018-03-15	⬇	-	⏱	MikroTik RouterOS < 6.41.3/6.42rc27 - SMB Buffer Overflow	Hardware	CoreLabs
2018-03-12	⬇	-	⏱	MikroTik RouterOS < 6.38.4 (x86) - 'Chimay Red' Stack Clash Remote Code Execution	Hardware	Lorenzo Santina
2018-03-12	⬇	-	⏱	MikroTik RouterOS < 6.38.4 (MIPSBE) - 'Chimay Red' Stack Clash Remote Code Execution	Hardware	Lorenzo Santina
2017-12-11	⬇	-	⏱	MikroTik 6.40.5 ICMP - Denial of Service	Hardware	FarazPajohan
2017-03-28	⬇	-	⏱	MikroTik RouterBoard 6.38.5 - Denial of Service	Hardware	FarazPajohan
2017-03-05	⬇	-	⏱	MikroTik Router - ARP Table OverFlow Denial Of Service	Hardware	FarazPajohan
2016-05-16	⬇	⚠	⏱	Web Interface for DNSmasq / Mikrotik - SQL Injection	PHP	hyp3rlinx
2013-09-03	⬇	-	⏱	MikroTik RouterOS - sshd (ROSSSH) Unauthenticated Remote Heap Corruption	Hardware	kingcope
2013-04-22	⬇	⚠	✔	Mikrotik Syslog Server for Windows 1.15 - Denial of Service (Metasploit)	Windows	xis_one
2012-05-01	⬇	-	⏱	Mikrotik Router - Denial of Service	Hardware	PoURaN
2008-09-05	⬇	-	✔	MikroTik RouterOS 3.13 - SNMP write (Set request)	Hardware	ShadOS
2008-02-04	⬇	-	✔	MikroTik RouterOS 3.0 - SNMP SET Denial of Service	Hardware	ShadOS

参考情報：https://goo.gl/pyALRG

ROUTEROSが晒される脅威2

- これらは、RouterOS自体の脆弱性であり、基本的なセキュリティ設定を行っておけば大きな問題になりにくい。
- 基本的な設定とは何か？
- **RouterOSに備えられている「Quick Set」を使用するだけで十分か？**

ROUTEROSが晒される脅威3

- 「Quick Set」だけでは基本的なFirewallの設定しかされない
- 幾つかの設定は自分で環境に合わせて設定するようにしましょう

行っておくべきセキュリティ設定 / Security settings

行っておくべきセキュリティ設定

- Manual:IP/Firewall/Filter - MikroTik Wiki
  https://wiki.mikrotik.com/wiki/Manual:IP/Firewall/Filter#Basic_examples
- Manual:IP/Services - MikroTik Wiki
  https://wiki.mikrotik.com/wiki/Manual:IP/Services
- Manual:SNMP - MikroTik Wiki
  https://wiki.mikrotik.com/wiki/Manual:SNMP#Reboot
- Manual:Router AAA - MikroTik Wiki
  https://wiki.mikrotik.com/wiki/Manual:Router_AAA

FIREWALL設定

- RouterOS自体はLinux kernelを利用したカスタムOS
- IP Firewallはよく見ると、Linuxで使用されるiptablesそのまま
  - Webに掲載されいるiptables設定を参考にするとよい
  - ただし、問題がないことを確認すること
- DNS attack対策

DNS ATTACK対策

- allow-remote-requestsをyesにしている場合、RouterOSを境界にどこからの応答にも返答してしまう

```
add action=drop chain=input comment="defconf: drop all not coming from LAN" in-interface-list=!LAN
```

- 上記の設定は入っているはずですが、以下の設定を明示的に設定しておく方が無難です

```
add action=drop chain=input comment="Block DNS" dst-port=53 protocol=udp in-interface=all-ppp
add action=drop chain=input comment="Block DNS" dst-port=53 protocol=tcp in-interface=all-ppp
```

SERVICEのアクセス設定1

- 以下のような感じで、最初はアクセス制御されていない

```
[admin@MikroTik] /ip service> print
Flags: X - disabled, I - invalid
 #    NAME            PORT ADDRESS
CERTIFICATE
 0    telnet           23
 1    ftp              21
 2    www              80
 3    ssh              22
 4 XI www-ssl          443                                    none
 5    api              8728
 6    winbox           8291
 7    api-ssl          8729                                   none
```

- 必要ないものはdisabledに、そうでないものは許可するアドレスを設定する

SERVICEのアクセス設定2

```
/ip service
set telnet disabled=yes
set ftp address=192.168.88.0/24 disabled=yes
set www address=192.168.88.0/24
set ssh address=192.168.0.0/16
set api disabled=yes
set winbox address=192.168.88.0/24,192.168.99.0/24
set api-ssl disabled=yes
```

- デフォルトでは、FTPやTELNET、APIなどが有効になっている
- SSH、www、winboxはPublicなどからのアクセスが行われないようにする
- アクセス制限するアドレスは複数設定できる
- WinboxのPortはbotなどに狙われている

SNMPのアクセス設定

- SNMPは最初は無効になっている
- 使用するときは、community設定を気を付ける
- アクセスできる範囲を限定する
- できれば認証を使用するようにする
- 認証プロトコルや暗号化プロトコルはSHA-1やAESをなるべく使用する

```
/snmp community
set addresses=192.168.88.0/24 authentication-password="" authentication-
protocol=MD5 encryption-password="" encryption-protocol=DES name=public
read-access=yes security=none write-access=no
```

ユーザー設定1

- デフォルトはadminのパスワードなし**(危険！)**
- パスワードを設定する
- adminという名前は狙われるので、別のユーザー名のユーザーを作成する
- adminは削除、またはdisabledにする
- Address設定を行い、ログインできるアクセス範囲を限定する
- 各種機能をpolicyで設定できる
- 上記のpolicyを活用し、権限を分離したユーザーグループを作成すると良い

ユーザー設定2

- LANからの接続に限定したもの

```
add address=192.168.0.0/16 disabled=no group=full name=kometchtech
```

- Ssh、write、policy、winboxの権限だけを付与したグループ

```
add name=test policy="ssh,write,policy,winbox,local" skin=default
```

- policyはたくさんあるので、公式Wikiを参照すること
  - Manual:Router AAA - MikroTik Wiki
    https://wiki.mikrotik.com/wiki/Manual:Router_AAA#Properties

その他1

- **Country block**
  - Country IP ranges
    http://www.iwik.org/ipcountry/
  - IP-Firewall-Address-List Generator
    https://mikrotikconfig.com/firewall/
- 今のところIPv4のものしか見つからない
- 更新中CPUを多く消費する
- Address-listはそのまま設定すると、NANDに書き込まれることになる
  - 書き換えを前提とすると、NANDの寿命が大幅に少なることが懸念される
  - Timeoutを設定するとメモリに展開される→**NANDへの影響が少ない！**

その他2

- **Blacklist filter**
- 広告やspybot、HijackやMalwareなどへの接続を防ぐ
  - mikrotikfilters.com (subscriptionへの移行が検討されている) https://forum.mikrotik.com/viewtopic.php?f=9&t=98804
  - Domain Blacklists - For Squid Proxy, and other web filtering platforms. https://www.squidblacklist.org/
  - blocklister.gefoo.org/ https://blocklister.gefoo.org/

その他3

- 必要のないパッケージを無効化し、機能を限定するようにしましょう。
  - 無線LAN機能を使用しないのであれば、WirelessをdisabledにIPv6を使用しないのであれば、ipv6をdisabledに
  - 無線LAN-APやSwitchとして使用するのであれば、pppをdisabledに
- 管理しないがゆえに脆弱性を放置することにもなりますし、無効化することでリソースの節約にもつながります。

参考情報 / for your reference

FOR YOUR REFERENCE1

- Vault7 – Home
  https://wikileaks.org/ciav7p1/
- Vault 7 – Wikipedia
  https://en.wikipedia.org/wiki/Vault_7
- 「自動車をハッキングして暗殺する」「テレビで部屋の会話を録音する」などCIAの極秘諜報作戦の実態を暴露する機密資料「Vault 7」をWikiLeaksが放出 – GIGAZINE
  https://gigazine.net/news/20170308-wikileaks-vault-7/
- Statement on Vault 7 document release - MikroTik
  https://forum.mikrotik.com/viewtopic.php?t=119308
- Exploit Database Search
  https://goo.gl/pyALRG

FOR YOUR REFERENCE2

- MikroTik Wiki
  https://wiki.mikrotik.com/wiki/Main_Page
- MikroTik - Forum index
  https://forum.mikrotik.com/
- Routerboard User Group Portal Site
  https://www.rb-ug.jp/

ご清聴ありがとうございました / Thank you！