关于MSR路由器遭受网络攻击造成版本丢失的经典案例

王喆兴 2018-01-03 发表

MSR路由器出现断电之后无法正常启动的问题，该问题原因有可能为设备受到网络黑客攻击，将设备flash格式化导致版本丢失，无法正常启动。

问题现象包括但不仅限于设备启动后，SYS指示灯黄色常亮，以太网接口指示灯灭（接口已经正确连接网线）。通过Console口登录设备命令行，可以看到设备在启动过程中，提示“Application program does not exist”信息。以某局点MSR2600设备为例，该启动输出信息如下图所示：

```
********************************************************************************
*                                                                              *
*                  H3C MSR26-00 BootWare, Version 5.40                         *
*                                                                              *
********************************************************************************
Copyright (c) 2004-2017 New H3C Technologies Co., Ltd.

Compiled Date       : Apr 25 2017
CPU ID              : 0x8
CPU L1 Cache        : 32KB
CPU L2 Cache        : 256KB
Memory Type         : DDR3 SDRAM
Memory Size         : 512MB
Memory Speed        : 667MHz
Flash Size          : 256MB
CPLD Version        : 1.0
PCB Version         : 2.0


BootWare Validating...
Application program does not exist.
BootWare password: Not required. Please press Enter to continue.

Password recovery capability is enabled.
Note: The current operating device is flash
Enter < Storage Device Operation > to select device.
```

MSR路由器遭受到网络攻击，攻击者破解了登录账号，登录MSR路由器删除了软件版本，进而导致设备断电之后无法重新启动的问题。

如下图，设备保存的log日志显示，存在大量的公网IP地址尝试登陆设备，采用的攻击手法为撞库攻击（黑客通过收集网络设备常用的用户名和密码，生成对应的字典表，然后尝试批量登陆网络中的设备，得到一系列可以登录的用户）。

```
======================================================
  ===============display logbuffer===============
======================================================
Logging buffer configuration and contents:enabled
Allowed max buffer size : 1024
Actual buffer size : 512
Channel number : 4 , Channel name : logbuffer
Dropped messages : 0
Overwritten messages : 180242
Current messages : 512

%Jan 16 02:37:43:209 2013 HACKED SC/6/SC_AAA_LAUNCH: -AAAType=AUTHEN-
AAAScheme= local-Service=login-UserName=support@system  AAA launched.
%Jan 16 02:37:43:209 2013 HACKED LS/5/LS_AUTHEN_FAILURE: -AccessType=login-
UserName=support; Authentication is failed. User not found.
%Jan 16 02:37:43:210 2013 HACKED SHELL/5/SHELL_LOGINFAIL:  TELNET user
support failed to log in from 81.7.138.27 on VTY0.
%Jan 16 02:37:47:209 2013 HACKED SC/6/SC_AAA_LAUNCH: -AAAType=AUTHEN-
AAAScheme= local-Service=login-UserName=enable@system  AAA launched.
%Jan 16 02:37:47:210 2013 HACKED LS/5/LS_AUTHEN_FAILURE: -AccessType=login-
UserName=enable; Authentication is failed. User not found.
%Jan 16 02:37:47:210 2013 HACKED SHELL/5/SHELL_LOGINFAIL:  TELNET user
enable failed to log in from 81.7.138.27 on VTY0.
%Jan 16 02:37:48:361 2013 HACKED SC/6/SC_AAA_LAUNCH: -AAAType=AUTHEN-
AAAScheme= local-Service=login-UserName=shell@system; AAA launched.
```

攻击者通过破解登陆账号和密码，登陆到设备上，修改设备系统名称，并且格式化了设备的Flash，由于设备的软件版本就存储在Flash中，这就导致了设备软件版本丢失，下次无法完成启动。

```
==========================================================
  ===============all history command===============
==========================================================

  01/15/2013 07:21:55  vt0   50.81.78.96     admin
  Cmd:super password simple ******

  01/15/2013 07:21:55  vt0   50.81.78.96     admin
  Cmd:sysname HACKED

  01/15/2013 07:21:55  vt0   50.81.78.96     admin
  Cmd:router id 1.2.3.4

  01/15/2013 07:21:54  vt0   50.81.78.96     admin
  Cmd:system-view

  01/15/2013 07:21:50  vt0   50.81.78.96     admin
  Cmd:format flash:
```

已经遇到该问题的用户，可以在MSR路由器命令行BootWare菜单下上传软件版本并重启设备。建议所有MSR路由器的用户按照如下方案配置MSR路由器加强安全防范。

禁止设置登录用户的认证方式为不认证，建议设置登录用户的认证方式为Scheme（用户名+密码）认证，该认证方式也是MSR路由器出厂情况下登录用户默认的认证方式。

MSR路由器出厂情况下配置了默认的登录账号，强烈建议修改密码或者直接删除该账号并重新配置账号，否则容易遭到非法用户的破解登录。

如果用户无需在外网登录管理MSR路由器，建议配置访问控制列表，对允许登录MSR路由器的IP地址进行限制。

MSR路由器通过BootWare升级软件版本

MSR V5路由器通过BootWare升级软件版本步骤（http://help.h3c.com/robot/p4data/fd69e65d30944f84a3ce1fdeff71d7fe/）

MSR V7路由器通过BootWare升级软件版本步骤（http://help.h3c.com/robot/p4data/52364944afa5492cb3275cf33610c5c5/）

MSR路由器修改admin用户密码配置

```
<H3C>system-view
[H3C]local-user admin       //MSR V7路由器对应的命令为local-user admin class manage
[H3C-luser-admin]password simple h3c_MSR930    //建议修改为复杂密码
[H3C-luser-admin]quit
```

MSR路由器限制登录用户IP地址配置

MSR V5路由器限制IP登录（http://help.h3c.com/robot/p4data/e3359db71d524ec2855287db28d3b625/）

MSR V7路由器限制IP登录（http://help.h3c.com/robot/p4data/eb62a6a1874b4df1992a650f57ad601c/）