

New issue

[Jump to bottom](#)

最新版v2.7存在拒绝服务漏洞 #2

Open 0xCaner opened this issue on Apr 23 · 0 comments

0xCaner commented on Apr 23 · edited

漏洞测试系统为:

360V6 IPQ6018/AP-CP03-C1

OpenWrt R22.3.18 / LuCI Master (git-22.077.27812-84c894f)

The screenshot shows the OpenWrt LuCI web interface. The top navigation bar includes links for Status, System, Services, Network Storage, VPN, Network, and Logout. The main content area is titled '状态' (Status) and contains a table of system information. Below the table, there are sections for '内存' (Memory) and '接口' (Interfaces).

系统	
主机名	OpenWrt
主机型号	360V6 IPQ6018/AP-CP03-C1 (CpuMark : 20576.853378 Scores)
架构	ARMv8 Processor x 4 (1320MHz, 60.0°C)
固件版本	OpenWrt R22.3.18 / LuCI Master (git-22.077.27812-84c894f)
内核版本	4.4.60
本地时间	Sat Apr 23 03:31:56 2022
运行时间	5h 59m 33s
平均负载	0.01, 0.03, 0.01
CPU 使用率 (%)	0%

内存

可用数	120 MB / 406 MB (29%)
已缓存	9 MB / 406 MB (2%)

接口

eth0	eth1	eth2	eth3

版本v2.7(最新版):

```
root@OpenWrt:~# /tmp/adbyby/adbyby
Version = 2.7
config file= /tmp/adbyby/adhook.ini
THIS IS DEAMON MODE!
run shell /tmp/adbyby/adbybyfirst.sh now!
Adbby Start Success !
```

漏洞触发方式:

通过访问http://【路由ip】:8118触发

效果:



该网页无法正常运行

ddns.0xcaner.top 未发送任何数据。

ERR_EMPTY_RESPONSE

重新加载

路由器 - root@OpenWrt: ~ - Xshell 7 (Free for Home/School)

文件(F) 编辑(E) 查看(V) 工具(T) 选项卡(B) 窗口(W) 帮助(H)

ssh://root:*****@192.168.1.1:22

要添加当前会话，点击左侧的箭头按钮。

1 路由器

tcp	0	0	59.55.253.156:46411	59.55.253.156:8118	ESTABLISHED	12510/adbbyby
tcp	0	0	59.55.253.156:8118	59.55.253.156:47821	ESTABLISHED	12510/adbbyby
tcp	0	0	59.55.253.156:8118	59.55.253.156:46732	ESTABLISHED	12510/adbbyby
tcp	0	0	59.55.253.156:8118	59.55.253.156:46216	ESTABLISHED	12510/adbbyby
tcp	0	0	59.55.253.156:46436	59.55.253.156:8118	ESTABLISHED	12510/adbbyby
tcp	0	0	59.55.253.156:8118	59.55.253.156:46342	ESTABLISHED	12510/adbbyby
tcp	0	0	59.55.253.156:46078	59.55.253.156:8118	ESTABLISHED	12510/adbbyby
tcp	0	0	59.55.253.156:47874	59.55.253.156:8118	ESTABLISHED	12510/adbbyby
tcp	0	0	59.55.253.156:8118	59.55.253.156:48020	ESTABLISHED	12510/adbbyby
tcp	0	0	59.55.253.156:47624	59.55.253.156:8118	ESTABLISHED	12510/adbbyby
tcp	0	0	59.55.253.156:46388	59.55.253.156:8118	ESTABLISHED	12510/adbbyby
tcp	0	0	59.55.253.156:8118	59.55.253.156:46188	ESTABLISHED	12510/adbbyby
tcp	0	0	59.55.253.156:47972	59.55.253.156:8118	ESTABLISHED	12510/adbbyby
tcp	0	0	59.55.253.156:47110	59.55.253.156:8118	ESTABLISHED	12510/adbbyby
tcp	0	0	59.55.253.156:46736	59.55.253.156:8118	ESTABLISHED	12510/adbbyby
tcp	0	0	59.55.253.156:46301	59.55.253.156:8118	ESTABLISHED	12510/adbbyby
tcp	0	0	59.55.253.156:8118	59.55.253.156:46608	ESTABLISHED	12510/adbbyby
tcp	0	0	59.55.253.156:46904	59.55.253.156:8118	ESTABLISHED	12510/adbbyby
tcp	0	0	59.55.253.156:8118	59.55.253.156:46645	ESTABLISHED	12510/adbbyby
tcp	0	0	59.55.253.156:46798	59.55.253.156:8118	ESTABLISHED	12510/adbbyby
tcp	0	0	59.55.253.156:46608	59.55.253.156:8118	ESTABLISHED	12510/adbbyby
tcp	0	0	59.55.253.156:47182	59.55.253.156:8118	ESTABLISHED	12510/adbbyby
tcp	0	0	59.55.253.156:47146	59.55.253.156:8118	ESTABLISHED	12510/adbbyby
tcp	0	0	59.55.253.156:8118	59.55.253.156:46142	ESTABLISHED	12510/adbbyby
tcp	0	0	59.55.253.156:8118	59.55.253.156:47384	ESTABLISHED	12510/adbbyby
tcp	0	0	59.55.253.156:8118	59.55.253.156:46392	ESTABLISHED	12510/adbbyby
tcp	0	0	59.55.253.156:8118	59.55.253.156:47724	ESTABLISHED	12510/adbbyby
tcp	0	0	59.55.253.156:47438	59.55.253.156:8118	ESTABLISHED	12510/adbbyby
tcp	0	0	59.55.253.156:8118	59.55.253.156:46538	ESTABLISHED	12510/adbbyby
tcp	0	0	59.55.253.156:8118	59.55.253.156:47247	ESTABLISHED	12510/adbbyby
tcp	0	0	59.55.253.156:8118	59.55.253.156:46214	ESTABLISHED	12510/adbbyby
tcp	0	0	59.55.253.156:8118	59.55.253.156:47842	ESTABLISHED	12510/adbbyby
tcp	0	0	59.55.253.156:46652	59.55.253.156:8118	ESTABLISHED	12510/adbbyby
tcp	0	0	59.55.253.156:8118	59.55.253.156:46252	ESTABLISHED	12510/adbbyby

ssh://root@192.168.1.1:22

SSH2 xterm 155x34 34,17 1 会话 CAP NUM

状态

系统

主机名	OpenWrt
主机型号	360V6 IPQ6018/AP-CP03-C1 (CpuMark : 20576.853378 Scores)
架构	ARMv8 Processor x 4 (1800MHz, 65.0°C)
固件版本	OpenWrt R22.3.18 / LuCI Master (git-22.077.27812-84c894f)
内核版本	4.4.60
本地时间	Sat Apr 23 17:32:24 2022
运行时间	0h 8m 44s
平均负载	1.75, 0.97, 0.43
CPU 使用率 (%)	55%

内存

可用数	<div><div></div>131 MB / 406 MB (32%)</div>
已缓存	<div><div></div>19 MB / 406 MB (4%)</div>

接口

<div><div>eth0</div><div></div><div>1000Mb/s 全双工</div></div>	<div><div>eth1</div><div></div><div>100Mb/s 全双工</div></div>	<div><div>eth2</div><div></div><div>10Mb/s 半双工</div></div>	<div><div>eth3</div><div></div><div>10Mb/s 半双工</div></div>
---	--	--	---

网络

IPv4 WAN 状态	<div><div></div><div>类型: pppoe 地址: 59.55.253.130 子网掩码: 255.255.255.255 网关: 59.55.252.1 DNS 1: 202.101.224.69 DNS 2: 202.101.226.69 已连接: 0h 8m 21s</div></div>
IPv6 WAN 状态	<div><div></div><div>未连接</div></div>
在线用户数	2
活动连接	<div><div></div>25128 / 65535 (38%)</div>

原：

状态

系统

主机名	OpenWrt
主机型号	360V6 IPQ6018/AP-CP03-C1 (CpuMark : 20576.853378 Scores)
架构	ARMv8 Processor x 4 (1056MHz, 62.0°C)
固件版本	OpenWrt R22.3.18 / LuCI Master (git-22.077.27812-84c894f)
内核版本	4.4.60
本地时间	Sat Apr 23 17:39:00 2022
运行时间	0h 15m 20s
平均负载	0.14, 0.54, 0.44
CPU 使用率 (%)	3%

内存

可用数	<div><div></div>151 MB / 406 MB (37%)</div>
已缓存	<div><div></div>18 MB / 406 MB (4%)</div>

接口

<div><div>eth0</div><div></div><div>1000Mb/s 全双工</div></div>	<div><div>eth1</div><div></div><div>100Mb/s 全双工</div></div>	<div><div>eth2</div><div></div><div>10Mb/s 半双工</div></div>	<div><div>eth3</div><div></div><div>10Mb/s 半双工</div></div>
--	---	--	--

网络

IPv4 WAN 状态	<div><div>pppoe-wan</div><div>类型: pppoe 地址: 59.55.253.130 子网掩码: 255.255.255.255 网关: 59.55.252.1 DNS 1: 202.101.224.69 DNS 2: 202.101.226.69 已连接: 0h 15m 2s</div></div>
IPv6 WAN 状态	<div><div></div><div>未连接</div></div>
在线用户数	2
活动连接	<div><div></div>942 / 65535 (1%)</div>

漏洞形成原因：

由于adbyby默认监听0.0.0.0的8118端口，导致攻击者可以从外部访问8118端口，或者还可以通过xss/csrf诱导内网用户访问，之后由于程序逻辑错误，最终导致自循环，产生大量连接，占用高额CPU

```
root@OpenWrt:~# netstat -anp
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State       PID/Program name
tcp        0      0 0.0.0.0:*                0.0.0.0:*              LISTEN      4196/
tcp        0      0 0.0.0.0:*                0.0.0.0:*              LISTEN      4968/
tcp        0      0 0.0.0.0:139              0.0.0.0:*              LISTEN      1540/smbd
tcp        0      0 0.0.0.0:80               0.0.0.0:*              LISTEN      1390/uhttpd
tcp        0      0 127.0.0.1:53             0.0.0.0:*              LISTEN      12684/dnsmasq
tcp        0      0 192.168.1.1:53           0.0.0.0:*              LISTEN      12684/dnsmasq
tcp        0      0 59.55.253.156:53        0.0.0.0:*              LISTEN      12684/dnsmasq
tcp        0      0 0.0.0.0:8118             0.0.0.0:*              LISTEN      12510/adbyby
tcp        0      0 0.0.0.0:3702             0.0.0.0:*              LISTEN      4968/wsdd2
tcp        0      0 0.0.0.0:22               0.0.0.0:*              LISTEN      1358/dropbear
tcp        0      0 127.0.0.1:5335           0.0.0.0:*              LISTEN      4038/pdnssd
tcp        0      0 127.0.0.1:6010           0.0.0.0:*              LISTEN      23097/dropbear
tcp        0      0 0.0.0.0:443              0.0.0.0:*              LISTEN      1390/uhttpd
tcp        0      0 0.0.0.0:445              0.0.0.0:*              LISTEN      1540/smbd
tcp        0      1 192.168.1.1:443          192.168.1.100:2382     LAST_ACK    -
tcp        0      0 192.168.1.1:443          192.168.1.100:2383     FIN_WAIT2   -
tcp        0      0 59.55.253.156:445        192.168.1.100:4313     ESTABLISHED 22201/smbd
tcp        0      0 192.168.1.1:22          192.168.1.100:1034     ESTABLISHED 23097/dropbear
```

```
root@OpenWrt:~# iptables -t nat -nl
Chain PREROUTING (policy ACCEPT)
target     prot opt source                destination
SS_SPEC_WAN_AC tcp -- 0.0.0.0/0              0.0.0.0/0              /* _SS_SPEC_RULE_ */
ADBYBY     tcp -- 0.0.0.0/0              0.0.0.0/0              tcp dpt:80
REDIRECT   udp -- 0.0.0.0/0              0.0.0.0/0              udp dpt:53 redir ports 53
REDIRECT   tcp -- 0.0.0.0/0              0.0.0.0/0              tcp dpt:53 redir ports 53
prerouting_rule all -- 0.0.0.0/0              0.0.0.0/0              /* !fw3: Custom prerouting rule chain */
zone_lan_prerouting all -- 0.0.0.0/0              0.0.0.0/0              /* !fw3 */
zone_wan_prerouting all -- 0.0.0.0/0              0.0.0.0/0              /* !fw3 */
zone_wan_prerouting all -- 0.0.0.0/0              0.0.0.0/0              /* !fw3 */
zone_VPN_prerouting all -- 0.0.0.0/0              0.0.0.0/0              /* !fw3 */
zone_vpn_prerouting all -- 0.0.0.0/0              0.0.0.0/0              /* !fw3 */
```

```
Chain ADBYBY (1 references)
target     prot opt source                destination
RETURN     all -- 0.0.0.0/0              0.0.0.0/8
RETURN     all -- 0.0.0.0/0              10.0.0.0/8
RETURN     all -- 0.0.0.0/0              127.0.0.0/8
RETURN     all -- 0.0.0.0/0              169.254.0.0/16
RETURN     all -- 0.0.0.0/0              172.16.0.0/12
RETURN     all -- 0.0.0.0/0              192.168.0.0/16
RETURN     all -- 0.0.0.0/0              224.0.0.0/4
RETURN     all -- 0.0.0.0/0              240.0.0.0/4
RETURN     all -- 0.0.0.0/0              0.0.0.0/0              match-set adbyby_esc dst
RETURN     all -- 0.0.0.0/0              0.0.0.0/0              ! match-set adbyby_wan dst
RETURN     all -- 0.0.0.0/0              0.0.0.0/0              match-set music dst
REDIRECT   tcp -- 0.0.0.0/0              0.0.0.0/0              redir ports 8118
```

临时修复建议:

- 一：使用iptables或防火墙限制从外部访问8118端口
- iptables -A INPUT -p tcp -dport 8118 -i <eth0 你的所有物理接口> -j reject
- 二：关闭adbyby

OpenWrt

状态 ▾ 系统 ▾ 服务 ▾ 网络存储 ▾ VPN ▾ 网络 ▾ 退出

自动刷新 开

基本设置

高级设置

Plus+ 模式过滤的域名

不走代理的域名

域名黑名单

IP黑名单

用户自定义规则

广告屏蔽大师 Plus+（支持 AdGuardHome /Host / DNSMASQ 规则）

广告屏蔽大师 Plus + 可以全面过滤各种横幅、弹窗、视频广告，同时阻止跟踪、隐私窃取及各种恶意网站

Plus + 版本可以和 Adblock Plus Host 结合方式运行，过滤广告不损失带宽

Adbby Plus+ 运行中

启用 ☒

运行模式 Plus + 模式（只过滤列表内域名! ▾

规则状态

手动更新规则

上一次检查规则更新: 2022-04-23 17:24:36

正式版规则:2019-12-22 16:42:18

测试版规则:2020-01-29 16:56:51

客户端过滤模式设置

可以为局域网客户端分别设置不同的过滤模式（不过滤，全局过滤）。默认无需设置。

IP地址	过滤模式	排序
尚无任何配置		

添加

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

1 participant

