OpenWRT Security

```
OpenWrt 21.02.0, r16279-5cc0535800
```

List of Targets supports DM_Verity:

	Supported	OpenWRT	RDK-B	prpl
pinnacles (SDX75)	Yes	Yes (Only on EMMC)	NO	
Kobuk (sdx85)	NO			

MBB Linux Security:

LinuxSecurity-MBB.pptx

Overview:

Will cover all the security feature that are planned for OpenWrt stack , There could be bit divergence in deployment from program to program based on memory or other PoR of the product here the info is in generic and mostly applicable to Pinnacles and its derivatives.

List of FRs by Security team :

- **FR47084:Provide Kernel and BSP binary protection**
- **FR52908:SELinux support**
- **FR52909:Deprivilege root processes**
- **FR83278:Support for ujail and capabilities**
- **Planned for DM-Verity (Dependent on overlayfs + other build support from platform team)**

List of PRs by Security team :

FR47084 : Provide Kernel and BSP binary Protection :

This FR is of two parts kernel-hardening and user space binary protection enablement .

For Pinnacles

SI OWRT.PRODUCT.2.0

PL : Pinnacles.LE.1.0

CPU : QuadCore A55 subsystem working in 64bit mode.

Kernel : its going to be with KERNEL.PLATFORM.2.0 (Which is 5.15 kernel version) .

Defconfig : generic_csm_defconfig (based defconfig) + Selinux.cfg+overlayfs.cfg

Kernel Hardening flags expected to be from standard template :

Kernel Key Name	Enabled (Y/N)	comments
CONFIG_HAVE_STACKPROTECTOR	Y	Stack buffer overflow mitigation
CONFIG_CC_STACKPROTECTOR_STRONG	N	Stack buffer overflow mitigation (legacy) using : CONFIG_CC_HAVE_STACKPROTECTOR_SYSREG need to cross check
CONFIG_STACKPROTECTOR_PER_TASK	Y	Stack protector per task instead of a global stack protector variable enabled
CONFIG_STACKPROTECTOR_STRONG	Y	Stack buffer overflow mitigation enabled
CONFIG_SLAB_FREELIST_HARDENED	Y	safe Heap -Many kernel heap attacks try to target slab cache metadata and other infrastructure. This options makes minor performance sacrifices to harden the kernel slab allocator against common freelist exploit methods. Some slab implementations have more sanity-checking than others. applicable to 32 & 64 bit
CONFIG_SLAB_FREELIST_RANDOM	Y	Safe Heap - Randomizes the freelist order used on creating new pages. This security feature reduces the predictability of the kernel slab allocator against heap overflows. applicable to 32 & 64 bit
CONFIG_STRICT_KERNEL_RWX	Y	DEP feature - If this is set, kernel text and rodata memory will be made read-only, and non-text memory will be made non-executable. This provides protection against certain security exploits (e.g. executing the heap or modifying text)
CONFIG_ARCH_HAS_STRICT_KERNEL_RWX	Y	W+X can lead to attacks , So map the regions with RO+X applicable to 32 & 64 bit
CONFIG_STRICT_MODULE_RWX	Y	DEP feature - If this is set, module text and rodata memory will be made read-only, and non-text memory will be made non-executable. This provides protection against certain security exploits (e.g. writing to text) CONFIG_STRICT_MODULE_RWX is enabled applicable to 32 & 64 bit
CONFIG_RANDOMIZE_BASE	Y	Kernel Address Space Layout Randomization (KASLR), arm32 does not support ASLR
CONFIG_CPU_SW_DOMAIN_PAN	N	Privileged Access Never (PAN) emulation (32-bit version). Not needed if HW PAN is used (ARM v8.1 and above) Pinnacles is ARM v8.2(A55) **so not needed .**
CONFIG_ARM64_SW_TTBR0_PAN	N	Privileged Access Never (PAN) emulation (64-bit version). Not needed if HW PAN is used (ARM v8.1 and above) Pinnacles is ARM v8.2(A55) **so not needed .**
CONFIG_ARM64_EPAN	N	Enhanced Privileged Access Never (EPAN) allows Privileged Access Never to be used with Execute-only mappings. Previous PAN implementation were for were read/exec, read, shared/exec etc. This one adds exec only support. The feature is detected at runtime, and will remain disabled if the cpu does not implement the feature.
CONFIG_ARM64_PAN	N	Privileged Access Never (PAN) feature Pinnacles is ARM v8.2(A55) **so not needed** .
CONFIG_ARM64_UAO	N	User access override -Ensures userspace does indeed have permissions to the buffer passed to kernel. copy_to_user() et al to use user-space memory permissions. Removed in 5.15 Kailua, ref: https://patchwork.kernel.org/project/linux-arm-kernel/patch/20170109181402.12883-1-james.morse@arm.com/#19982385 The feature is detected at runtime, the kernel will use the regular load/store instructions if the cpu does not implement the feature. 5.15 and later kernel don't need explicitly enabling . 32 bit not applicable

CONFIG_HAVE_ARCH_SECCOMP_FILTER	Y	support for system call whitelisting
CONFIG_SECCOMP	Y	System call whitelisting enabled
CONFIG_SECCOMP_FILTER	Y	Filter sys calls auto enabled with CONFIG_HAVE_ARCH_SECCOMP_FILTER && CONFIG_SECCOMP && CONFIG_NET enabled
CONFIG_DEBUG_FS	Y	Kernel config option can be present, but user variant must not mount debugfs **Baseport team agreed to remove this access Need to follow**
CONFIG_HARDENED_USERCOPY	Y	Hardened usercopy exposes incorrect bounds checking when copying data to/from user space. These should be fixed like any other memory corruption bugs.
CONFIG_HAVE_HARDENED_USERCOPY_ALLOCATOR	Y	support for Hardened usercopy
CONFIG_HARDENED_USERCOPY_PAGESPAN	Y	3.18+ **Need to revalidate**
CONFIG_FORTIFY_SOURCE	N	Fortify Sources **Need to revalidate**
CONFIG_ARCH_HAS_FORTIFY_SOURCE	Y	is enabled
CONFIG_SECURITY_PERF_EVENTS_RESTRICT	N	Restrict perf events This is a Google added feature that seems to have been removed from later kernels now perf events can be controlled by SELinux so if want to capture the perf events SELinux rules are needed to **so not needed** .
CONFIG_LSM_MMAP_MIN_ADDR=32768	Y	32768 is default value for ARM core , is the lowest address that can be mapped is protected from userspace access and allocations.
CONFIG_THREAD_INFO_IN_TASK	Y	Move thread_info off of the task stack. Refer to https://lwn.net/Articles/700782/ enabled

User space Hardening flags :

Logging Restrictions: kptr_restrict/ dmesg_restrict -

- Reduces information leak by not printing kernel address in logs.

Debug build with have this kptr_restrict valure to 0 (which will display the kernel pointer) . For user/production build we are expecting this to be 2 restricting display of kernel pointers

```
/ # cat /proc/sys/kernel/kptr_restrict
0
/ # cat /proc/sys/kernel/dmesg_restrict
0
```

FR52908: SELinux Enablement :

SELinux:

As per of security compliance we want Pinnacles and above time -lined target to be in enforce mode .

Where expectation is tech team to document all the required sepolicy in line BU time lines /Based on the feature enablement .

SELinux is expected be in enforce mode from Day-one of BU lab any tech team which had hard dependency and not able to be meet are free to move to permissive (only for there service) with agreement with PE and security team .

For understanding of SELinux on Openwrt you can refer the earlier presented session and FAQ in the links below for additional reading please

https://github.com/SELinuxProject/cil/wiki/

SELinux -FAQ

Status on Pinnacles :

1. SElinux is enforce and all the requested changes are part of build .
2. SELinux labeling at build time (WIP ETA 20 Nov) and post boot are done and should be blocker for tech teams

How to check is selinux is enforce ?

In adb shell / Serial console : " getenforce " this will show the current status of the device .

Permission which are not to be used

execmod

execmem

relabel

mount

setuid

setgid

dac_search /override

write to procfs /sysfs by userspace application until unless its justified and agreed with security team .

Handling of execmod/execmem

There is no explicitly flag switch /target check in sepolicy code if there is a big divergence we might think of so make sure to add commets in the code if needed we should be able to separate this .

Following permission are not allowed :

1. *execmod*
2. *execmem*

which are to be address by compiler flags like -fpic and -fpie following is one example for now going fwd platform team will share a global way of passing cflag/ ldflags .

https://review-android.quicinc.com/#/c/4183989/

Handing of dac_serach/dac_override :

This issue should not be addressed by adding sepolicy rather you have to update the user group of your service .

Generally these are seen when file/folder/socket/devnode/,.... resource are not part of your services listed user /group so you can update the user /group /supplement group to the list .

Go through this document .

https://lukas-vrabec.com/index.php/2018/07/03/why-do-you-see-dac_override-selinux-denials/

Expectation from tech team :

Please get the required permission documented as part of the CIL file and get the features tested with enforce mode.

Current set of changes are making in global permissive we want you to check your module with enforce mode once the required policy are documented.

Please start adding the details of your services and dependents in the table below .

Tech team	PoC	Services /Init file	Bin /libs / sockets	CIL sample ready	Share the permissive logs to security	Comments
	VIJAYAN CHENGANNAGARI	diag-router				
		diagrebootapp				
		rmt-storage				
		QCMAP_con				
	Saurav Kumar	audio				
	Harikrishnan Hariharan	location				
	Dheeraj Kumar	qti and adpl				
	Aman Gupta	mbim				
		qcmap_cm				

For Migration of selinux policy from LE to OpenWRT you can follow this link OpenWrt Migration

example to just make dependent service to permissive while testing .

Change I4b17bc50: owrt: Adding permissive selinux mode for diag-router service | review-android.quicinc Code Review

FR52909 : Deprivilege Root

Expectation is services should start with it own UID / Group (non-Root) and always try to use the least privilege user/ group.

If this details are not given it will run the process as root where any security vulnerability in the code gives an attacker to exploit system.

Following is the confluence page which will give you details on how to add your own UID and GID.

FR52909:Deprivilege root processes

Now going fwd we expect the resources (file/folder ,socket..) also are going to be explicitly added with appropriate group and User.

Handling of insmod

We understand insmod need root permission , So platfrom team had suggest 2 approchs ,

In openwrt case :

a. you can use .init with out user and group and call the insmod (Please no other operations should be done)

b. You can group the ko in sperate file as suggested in "External Kernel Module Template for Init scripts" but that sh should be only restricted to loading no other operation should be done in this .

In LE case :

You can have insmod in the .service file itself as show below as .service will be root it should not have problem in loading .

```
ExecStart=/sbin/insmod /usr/lib/modules/tz_log.ko
```

For dynamic module (module which are loaded and unloaded at run time) we want to have dedicated process to do this and check with security team on this .

FR83278: Support for ujail and capabilities

Please visit following link

Enabling service Capabilities in OWRT

DM-Verity

we are tracking verity effort in following page

DM_verity Support on OpenWRT

Support team :

rsiddoji, arukmang

supporting email : seandroid.support

Gerrit support :   owrt.sepolicy.approvers

Internal Resources :

Presentation on SELinux and all SDX75

(if above link is not working you can visit the home page of sdx75 -- Link

SELinux rule migration guide

FAQ

Link to sdx75 resources

User login restriction