



EMBEDDED
OPEN SOURCE
SUMMIT

Yocto Project/ OpenEmbedded Meets Security

Marta **Rybczynska**, Syslinbit

marta.rybczynska@syslinbit.com

#EMBEDDEDOSSUMMIT



EMBEDDED
OPEN SOURCE
SUMMIT

Embedded Linux Security: long time ago

```
login: root  
password: root
```



KA-SAT Network cyber attack overview

Viasat is providing an overview and incident report on the cyber-attack against the KA-SAT network, which occurred on 24 February 2022, and resulted in a partial interruption of KA-SAT's consumer-oriented satellite broadband service.

March 30, 2022 04:55 AM • Viasat, Inc.

Source: <https://news.viasat.com/blog/corporate/ka-sat-network-cyber-attack-overview>



reversemode
@reversemode

Viasat incident

I managed to dump the flash of two Surfbeam2 modems: 'attacked1.bin' belongs to a targeted modem during the attack, 'fw_fixed.bin' is a clean one. A destructive attack.

attacked1.bin		fw_fixed.bin	
A0	FFFF 57DD FFFF 56DD FFFF 55DD FFFF 54DD	1CA8AA0	0B02 310D 8D90 250C E112 C6C6 48E2 E670
B0	FFFF 53DD FFFF 52DD FFFF 51DD FFFF 50DD	1CA8AB0	6173 7364 E526 38C4 4D01 0208 2E6E 69CE
C0	FFFF 4FDD FFFF 4EDD FFFF 4DDDD FFFF 4CDD	1CA8AC0	0510 6000 6667 1F25 1985 C001 0000 0031
D0	FFFF 48DD FFFF 4ADD FFFF 49DD FFFF 48DD	1CA8AD0	C320 DD5D 0000 0003 0000 0008 0000 000F
E0	FFFF 47DD FFFF 46DD FFFF 45DD FFFF 44DD	1CA8AE0	483D 3885 0908 0000 882D 4288 A08A 07CE
F0	FFFF 43DD FFFF 42DD FFFF 41DD FFFF 40DD	1CA8AF0	6265 616D 2D68 6973 74FF FFFF 1985 C001
00	FFFF 3FDD FFFF 3EDD FFFF 3DDDD FFFF 3CDD	1CA8B00	0000 0035 C44D 1944 0000 0003 0000 000C
10	FFFF 38DD FFFF 3ADD FFFF 39DD FFFF 38DD	1CA8B10	0000 0000 4B3D 3885 0D00 0000 D544 44A7
20	FFFF 37DD FFFF 36DD FFFF 35DD FFFF 34DD	1CA8B20	1724 20CE 6265 616D 2D68 6973 742E 746D
30	FFFF 33DD FFFF 32DD FFFF 31DD FFFF 30DD	1CA8B30	70FF FFFF 1985 C002 0000 0044 A4EF 223E
40	FFFF 2FDD FFFF 2EDD FFFF 2DDDD FFFF 2CDD	1CA8B40	0000 0010 0000 0001 0000 81B6 0000 0000
50	FFFF 28DD FFFF 2ADD FFFF 29DD FFFF 28DD	1CA8B50	0000 0000 5745 E957 5745 E957 5745 E957
60	FFFF 27DD FFFF 26DD FFFF 25DD FFFF 24DD	1CA8B60	0000 0000 0000 0000 0000 0000 0000 0000
70	FFFF 23DD FFFF 22DD FFFF 21DD FFFF 20DD	1CA8B70	0000 0000 331C C8E1 1985 C001 0000 0038
80	FFFF 1FDD FFFF 1EDD FFFF 1DDDD FFFF 1CDD	1CA8B80	BAFC 65F9 0000 0003 0000 0000 0000 0010

From:
Hegel and
Guerro-Saade -
"Real 'Cyber War':
Espionage, DDoS,
Leaks, and
Wipers in the
Russian Invasion of
Ukraine"
Defcon 2022

AcidRain

Targeted Device(s)	Description
/dev/sd*	A generic block device
/dev/mtdblock*	Flash memory (common in routers and IoT devices)
/dev/block/mtdblock*	Another potential way of accessing flash memory
/dev/mtd*	The device file for flash memory that supports fileops
/dev/mmcblk*	For SD/MMC cards
/dev/block/mmcblk*	Another potential way of accessing SD/MMC cards
/dev/loop*	Virtual block devices

From:
Hegel and
Guerro-Saade -
“Real 'Cyber War':
Espionage, DDoS,
Leaks, and
Wipers in the
Russian Invasion of
Ukraine”
Defcon 2022

- Are your services running **lowest possible** permissions?
- Are your special devices (eg. flash) **protected from random services**?
- Do you **trace vulnerabilities** in your software stack?
- Can you **update** your software stack (without too much damage)?

Embedded Linux Security: Kittens!



**Product Liability Directive
(PLD) update**

Cyber Resilience Act (CRA)

Photo credits

<https://www.flickr.com/photos/crsan/2571204698> Christian Holmér CC BY 2.0



EMBEDDED
OPEN SOURCE
SUMMIT

Yocto Project/ OpenEmbedded Meets Security

Marta **Rybczynska**, Syslinbit

marta.rybczynska@syslinbit.com

#EMBEDDEDOSSUMMIT

- **PhD** in Telecommunications (Network Security)
- **20+ years in Open Source**, former Vice-President and Treasurer of KDE e.V.
- Currently focusing on **Open Source Supply Chain**
- Founder of Syslinbit, a company offering development and training, including **embedded security**



EMBEDDED
OPEN SOURCE
SUMMIT

Security Meets Yocto Project/OpenEmbedded

How do you **design secure devices** with Yocto Project/Open Embedded?

Phase 1: Creation

Phase 2: Configuration

Phase 3: Maintenance

Phase 1: Creation

Phase 2: Configuration

Phase 3: Maintenance

Follow best practices for YP

- Follow “What I wish I’d known about Yocto Project”
 - <https://docs.yoctoproject.org/dev/what-i-wish-id-known.html>
- Follow “Making images more secure”
 - <https://docs.yoctoproject.org/dev/dev-manual/securing-images.html>
- Use yocto-check-layer
 - Not only when applying to the Yocto Compatible Program
 - <https://docs.yoctoproject.org/test-manual/yocto-project-compatible.html#validating-a-layer>
- Read the docs - if you do not understand, ask!

Do NOT start from poky

- This is a common practice, but defaults not always safe
 - Example: debug-tweaks enabled
 - Example: DISTRO_FEATURES contain a little too much
- Instead: create your own distribution

Keep external layers unchanged

- Perform changes in .bbappend files in your own layers
- Will see why in phase 3: maintenance

Choose 3rd party layers carefully

- Make sure it follows best practices
 - yocto-check-layer is a good test
- Verify if it is up to date
 - Recent commits, support for latest releases
- Look into the code
 - Does it look correct?

Use meta-security

- recipes-scanners: various scanners for your distro
- recipes-compliance: verification of security policy
- recipes-kernel: Linux Security Modules, dm-verity...
- meta-security: various security tools

Phase 1: Creation

Phase 2: Configuration

Phase 3: Maintenance

Cut unneeded features

- Remove unneeded DISTRO_FEATURES

Example with poky master `13b646c0e167ca52f69c91be5538049b172015ac`

```
DISTRO_FEATURES="acl alsa bluetooth debuginfod ext2 ipv4 ipv6 pcmcia  
usbgadget usbhost wifi xattr nfs zeroconf pci 3g nfc x11 vfat seccomp  
opengl ptest multiarch wayland vulkan sysvinit pulseaudio  
gobject-introspection-data ldconfig"
```

- Production image should not contain debug tools (eg. nfs, gdb, compilers...)
- Review your dependencies list

When adding tools, follow (their) best practices

- Example: kubernetes or docker configuration is tricky

Unique passwords for devices

- See another presentation on this subject

Apply hardening

- Use separate users for each important service
- Compiler flags
`openembedded-core/meta/conf/distro/include/security_flags.inc`
- Lower permissions of files
 - `meta-security/meta-hardening`

Hardening Linux configuration

- Remove DEBUG_* features
- Remove subsystems you do not need
- Implement recommendations from the Kernel Self Protection Project
 - Example:
<https://gitlab.eclipse.org/eclipse/oniro-core/oniro/-/tree/kirkstone/meta-oniro-core/recipes-kernel/linux/linux>

Phase 1: Creation

Phase 2: Configuration

Phase 3: Maintenance

CVE-checking in 2022

- Possible to check the complete set of layers with “cve-check”
 - INHERIT += “cve-check”
- Using NVD format
<https://nvd.nist.gov/vuln/detail/CVE-????-????>
- Text or JSON output formats
- Image or complete build

Changes in 2023

- NVD database old format going down in September 2023 (*)
- CVE 5.0 format launched
 - <https://github.com/CVEProject/cvelist>

YP CVE checking changes in 2023

- New fetcher using NVD new format
 - master and mickledore: enabled by default
 - kirkstone, dunfell: not ported yet
- Work on management of kernel CVEs
 - Multiple issues per week, often missing information in NVD
- A proposal pending to rework CVE_CHECK_IGNORED



EMBEDDED
OPEN SOURCE
SUMMIT

Yocto Project/ OpenEmbedded Meets Security

Marta **Rybczynska**, Syslinbit

marta.rybczynska@syslinbit.com

#EMBEDDEDOSSUMMIT

Phase 1: Creation

Phase 2: Configuration

Phase 3: Maintenance

- More vulnerability fetchers
 - Kernel CVEs
- Kernel hardening v2
- Vulnerability checker and SPDX post-processing
- meta-hardening rework as a DISTRO_FEATURE



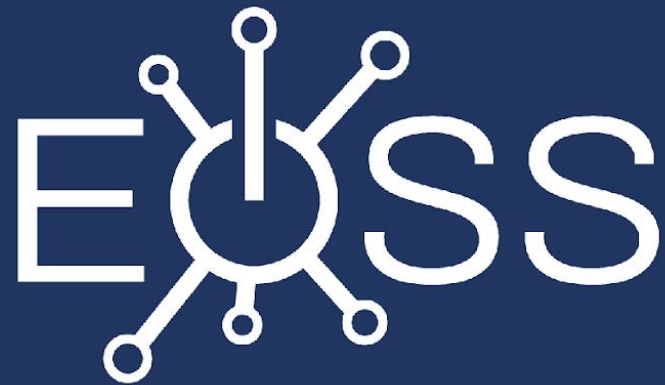
EMBEDDED
OPEN SOURCE
SUMMIT

Yocto Project/ OpenEmbedded Meets Security

Marta **Rybczynska**, Syslinbit

marta.rybczynska@syslinbit.com

#EMBEDDEDOSSUMMIT



EMBEDDED
OPEN SOURCE
SUMMIT