Yocto Project/OpenEmbedded Meets Security

Marta Rybczynska, Syslinbit
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.

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.
## AcidRain

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

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

- Are your services running **lowest possible** permissions?
- Are your special devices (e.g., 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
How do you **design secure devices** with Yocto Project/OpenEmbedded?
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](https://docs.yoctoproject.org/dev/what-i-wish-id-known.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](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
● Instead: create your own distribution
Do NOT perform direct changes to layers

- Perform changes in .bbappend files in your own layers
Choose 3rd party layers carefully

- Make sure it follows best practices
  - yocto-check-layers is a good test
- Verify if it is up to date
  - Recent commits, support for latest releases
Use meta-security
Phase 1: Creation
Phase 2: Configuration
Phase 3: Maintenance
Cut unneeded features

- Remove unneeded DISTRO_FEATURES
- 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
    - This one is included in poky!
- Lower permissions of files
  - meta-security/meta-hardening
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-????-?????](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](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
Phase 1: Creation
Phase 2: Configuration
Phase 3: Maintenance
• More vulnerability fetchers
  ○ Kernel CVEs
• Vulnerability checker and SPDX post-processing
• meta-hardening rework as a DISTRO_FEATURE
Yocto Project/OpenEmbedded Meets Security

Marta Rybczynska, Syslinbit

Embedded Open Source Summit 2023