Timesys University Webinar Series

Reduce Risk with RISC: Designing and Maintaining Secure Embedded Linux Devices with Advantech RISC Platforms

Session 1: Monitoring and patching security vulnerabilities throughout the embedded Linux product lifecycle

Today's Presenters:

Maciej Halasz
Vice President of Technology
Timesys

Jason Zhu
RISC Product Manager
Advantech

Theresa Kisha
Moderator
Timesys

Agenda

- **Is security important?**
- **Advantech-Timesys partnership**
- **Building secure devices with Advantech RISC Platforms**
- **Security in an embedded Linux device**
  - Security by design
  - Staying secure
- **Security vulnerabilities**
  - What are they?
  - Why do we care?
- **How do we keep Linux devices secure?**
- **Stay Secure – Solution for Security Vulnerability and Patch Notification**
  - Continuous security monitoring for your products
  - Vulnerability Push and Pull Notification
  - Patch Notification
  - BSP Maintenance

Giveaway!

Is security important?

Security – what does it mean?

- **Security — broad definition and broad understanding**
- **Secure — Protected, Defended, Guarded, Immune, Unassailable …**
- **In the embedded world**
  - Prevent unauthorized use of the device or data it collects, stores or transmits
  - Typical use of embedded devices:
    - Control unit eg. Car computer
    - Data collection eg. Measuring device
    - User access point eg. POS
    - Concentration node eg. Network hub
    - Many more
- **Security must be considered in products in all market segments including:**
  - Financial
  - Medical
  - Industrial
  - Automation
  - more

BUT WHY?

Jeep Cherokee Owners File Lawsuit Against Fiat Chrysler, Harman After Hackers Wirelessly Hijack Vehicle

By Mary Beth Quirk @marybethquirk August 5, 2015

Building secure devices with Advantech RISC Platforms

Embedded Linux & Android ARM Platform

Accelerating Your ARM Project Development

Presented by Jason Zhu

LET'S GROW
THE FUTURE TOGETHER.

The Key Factors for ARM Business Success

IoT Connectivity

- WISE-PaaS Built-in
- SUSI API Built-in

ADVANTECH WISE-PaaS IoT Software Platform

Kernel & Industrial Peripheral Modules

- Standardized BSP
- Advantech Loader
- Longevity Yocto & Android BSP Upgrade

Document | API | Tool

Driver | Kernel | Boot Loader

Timesys

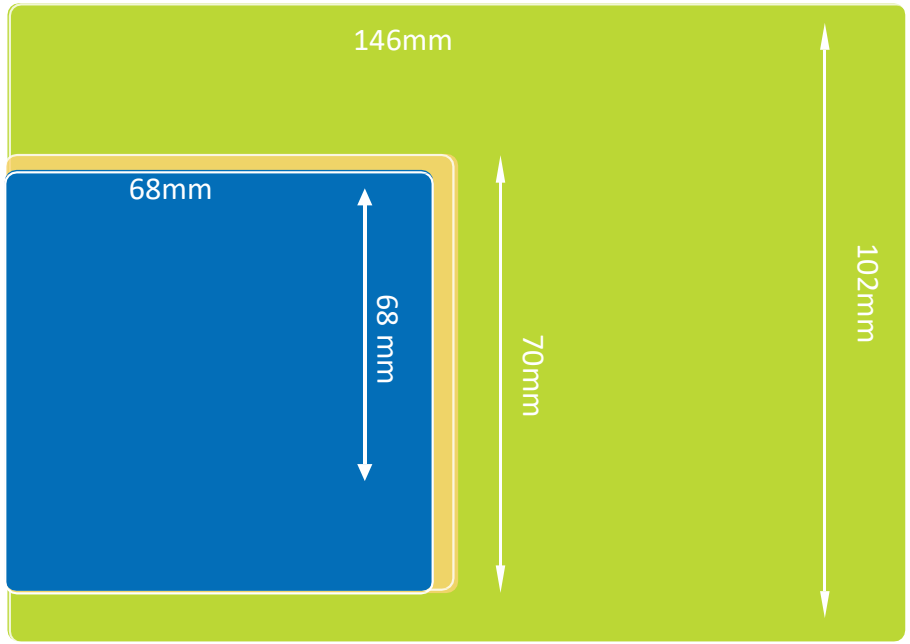
- Build Engine
- Custom OS
- Driver Porting
- Performance Tuning
- Vertical AP

- Security notification
- Secure Boot

Unified ARM Development Platform

- Optimal
- Configurable
- Compatible

Standardized Hardware Solutions



Advantech has been working with RISC technology for over 10 years beginning with MIPS. We think standardizing the form factor is a key factor in making RISC more popular. With this in mind, Advantech launched its COM (Computer on module), SBC (Single Board Computer) and RISC Development Kits into the market.

RTX (Advantech)
68mm x 68mm

Qseven
70mm x 70mm

3.5" SBC
146mm x 102mm

Computer On Modules

Computer On Module (COM) is a type of platform which tightly integrates all main components and is well proven and compatible. The modularized design helps developers quickly build their own carrier boards for their own unique application.

RTX	Qseven	Qseven	SMARC
ROM-3420	ROM-7420	ROM-7421	ROM-5420
▪NXP i.MX6 Cortex-A9 1GHz Dual/Quad core ▪Outstanding graphic performance ▪Designed for rugged applications	▪NXP i.MX6 Cortex-A9 1GHz Dual/Quad core ▪Cost effective module solution ▪Designed for networking and signage	▪NXP i.MX6 Cortex-A9 1GHz Dual Plus/Quad Plus ▪Strong multimedia performance ▪Designed for Kiosk and HMI	▪NXP i.MX6 Cortex-A9 SoC ▪ROM-DB5900 for easy integration and hardware design reference

Single Board Computers

Advantech has long developed its Single Board Computer (SBC) series of products, which come in standard form factors in compact sizes with rich I/O, extremely low power consumption, and easy expansion capabilities. This helps you to reduce your H/W design effort and speeds your time to market.

RSB-6410	RSB-4410	RSB-4411
▪Ni.MXXP6 Cortex-A9 1GHz Dual/Quad Core ▪Powerful multi-display capability, multiple I/O, and wireless connectivity ▪Designed for kiosks and IoT gateways	▪NXP i.MX6 Cortex-A9 1GHz Dual/Quad Core ▪Supports LVDS, VGA and HDMI display ▪Designed for signage applications	▪NXP i.MX6 Cortex-A9 1GHz Dual/Quad Core ▪Rich I/O and wide range temperature and power input support ▪Designed for HMI and industrial control

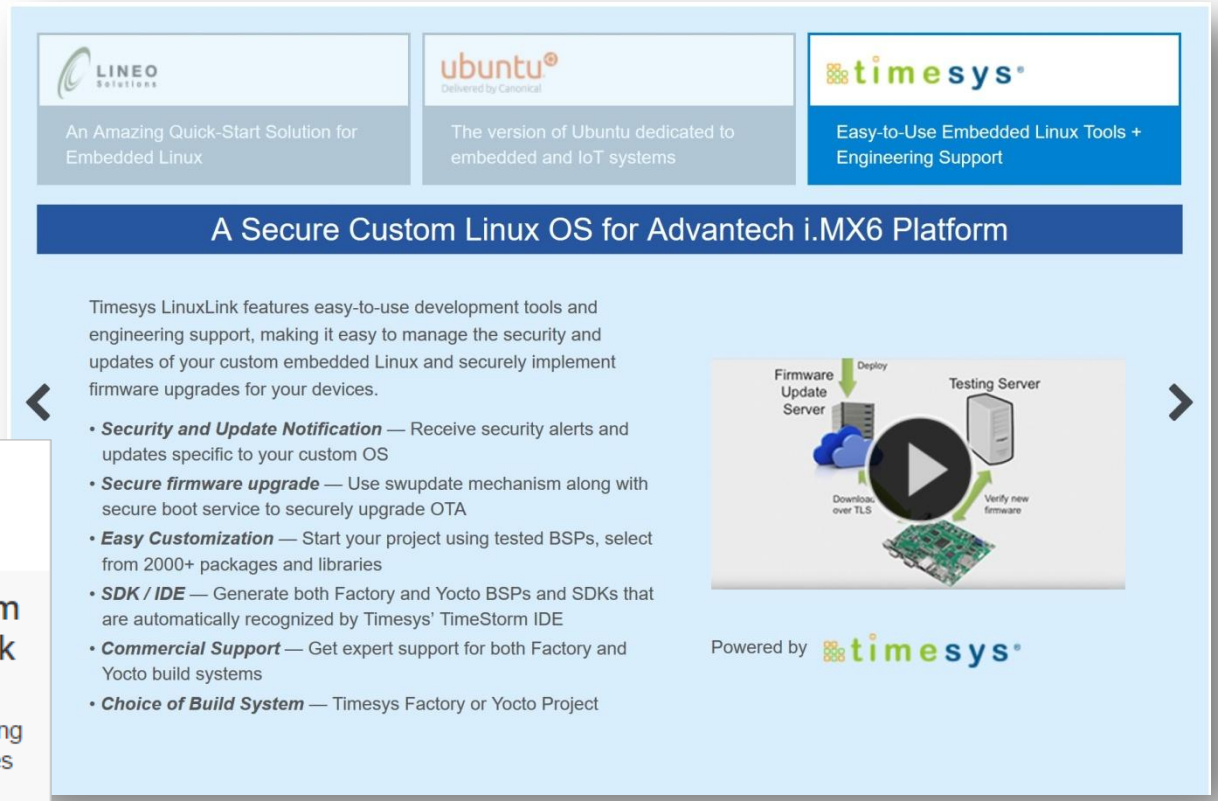
Not Just Eco-System Partner

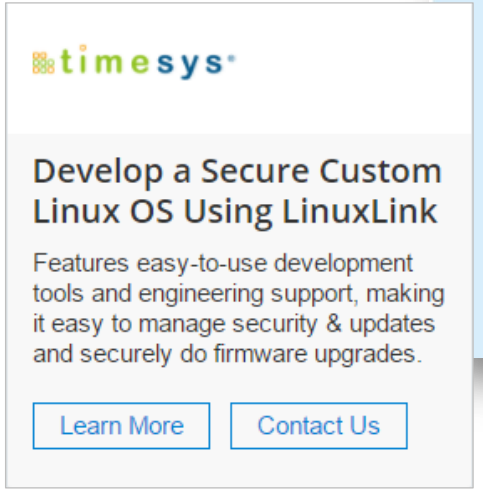
What Advantech Provides:
Latest and Greatest HW solution on different Arm form factor.
+ Longevity
+ Revision control
+ Design in services

What Timesys provides:
Easy-to-Use Embedded Linux Tools
+ Security solutions
+ Engineering Services
+ Support
= Accelerated Development Cycles

Advantech-Timesys partnership

- Advantech and Timesys offer a solution which provides state-of-the-art hardware with the Linux software that is easy to use in product development
- What customers can do:
  Develop Secure Custom Linux products with Advantech i.MX6 Platforms





- Support will address customers questions directly and specifically

Security in an embedded Linux device

Product security

200-node Connectivity

Reliable Mesh Network

Secure by Design

- Secure Boot
- Data at rest security
- Data in motion security
- Data in use security

Stay Secure

Threat Identified → Threat mitigated

Product development — 6-24 months

Product maintenance — 2-20 years

Release to the market

Security vulnerabilities

Common Vulnerabilities and Exposures

- **What is a CVE®?**
  - It is a publicly known cyber security issue
    http://cve.mitre.org

Common Vulnerabilities and Exposures

- **How does it work?**
  - When a possible security vulnerability is discovered, a CVE identifier is first created
  - CVE Numbering Authority (CAN) assigns a CVE ID and posts it on the CVE list on the CVE website

CVE entry includes:

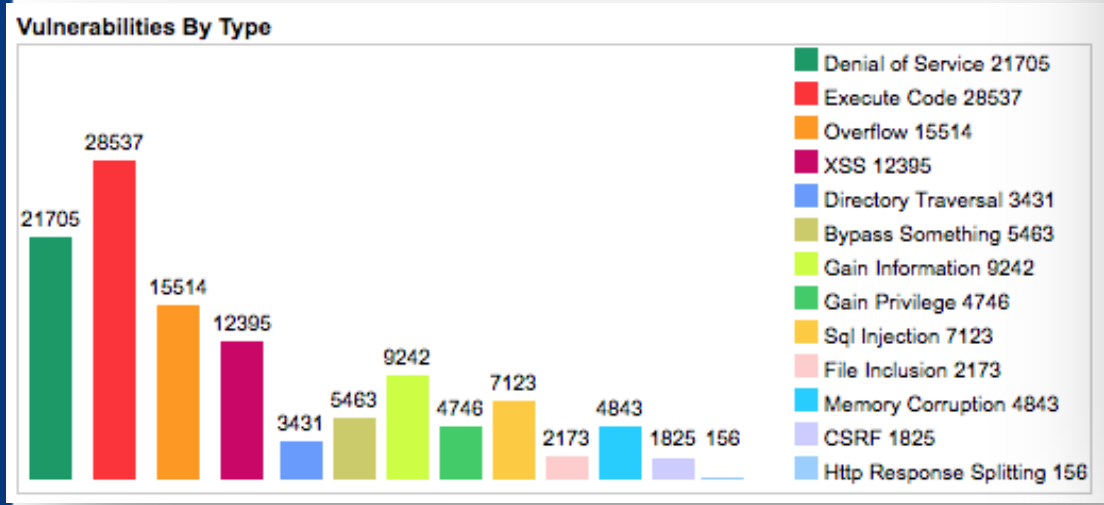
- CVE ID with four or more digits in the sequence number portion of the ID (i.e., "CVE-1999-0067", "CVE-2014-12345", "CVE-2016-7654321").
- Brief **description** of the security vulnerability or exposure.
- Any pertinent **references** (i.e., vulnerability reports and advisories).

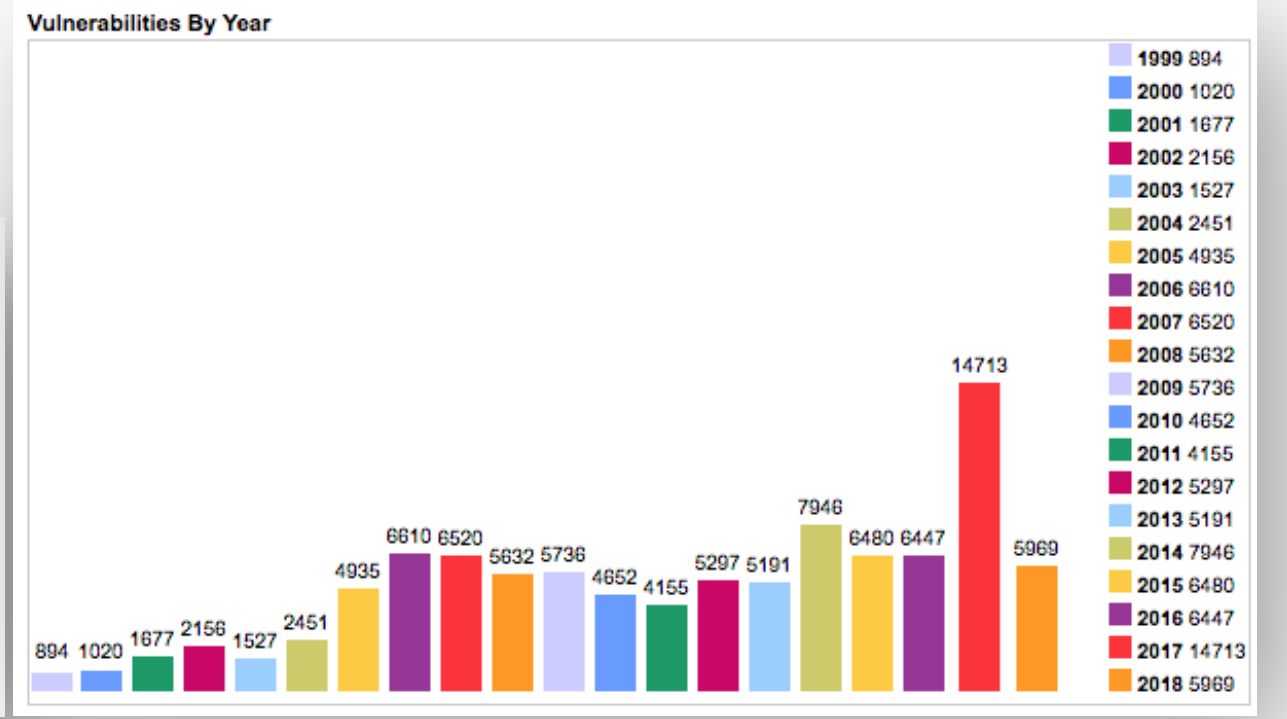
CVE Numbering Authority

- **CVE Numbering Authorities (CNAs) are organizations from around the world...**
- **87 organizations participating as CNAs**
  - MITRE Corporation
  - Google
  - Node.js
  - RedHat
  - Canonical
  - Qualcomm
  - Many more
- **Most of the organizations are vendors and projects**

Vulnerabilities are a growing trend

- **Reported vulnerabilities have reached 14000+ a year!!!**



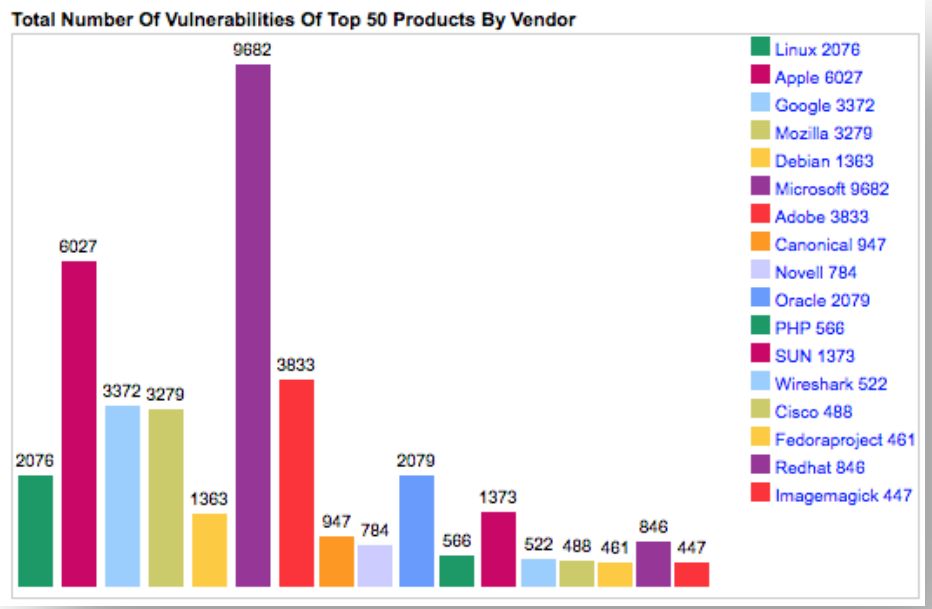


Source: cvedetails

- **How do we keep devices secure?**
  - Companies must integrate additional governance into development processes

CVE statistics

- **Many vulnerabilities reported for open source projects**



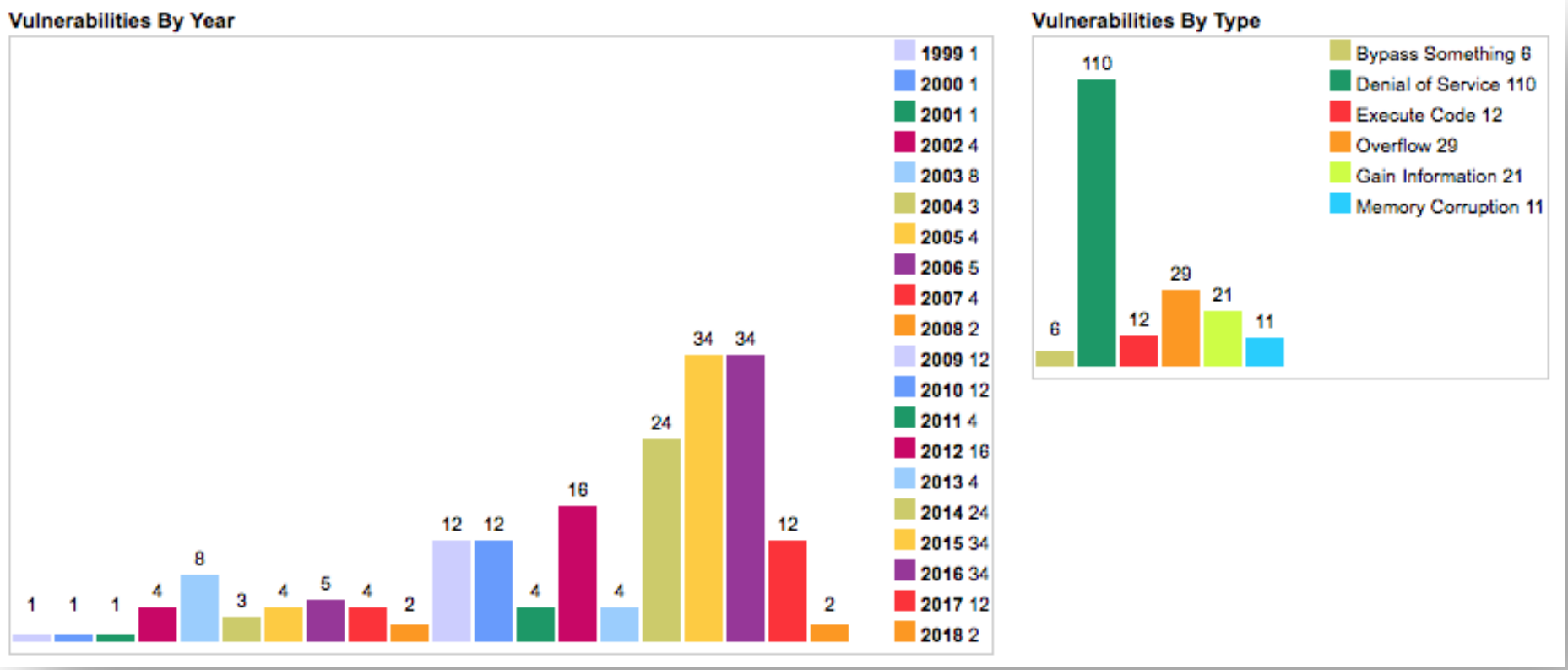
CVSS Score Distribution For Top 50 Products By Total Number Of "Distinct" Vulnerabilities

	Product Name	Vendor Name	Number of Total Vulnerabilities	# Of Vulnerabilities										Weighted Average
				0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9+	
1	Linux Kernel	Linux	2075	1	91	311	42	623	137	164	574	5	127	5.90
2	Mac Os X	Apple	2049	1	20	144	21	331	251	451	421	10	399	7.00
3	Android	Google	1825		2	39	11	346	162	129	361	24	751	7.90

Source: cvedetails

CVE statistics example — openssl

- 316 total number of vulnerabilities for the package
- 12 vulnerabilities found in 2017 alone



Source: cvedetails

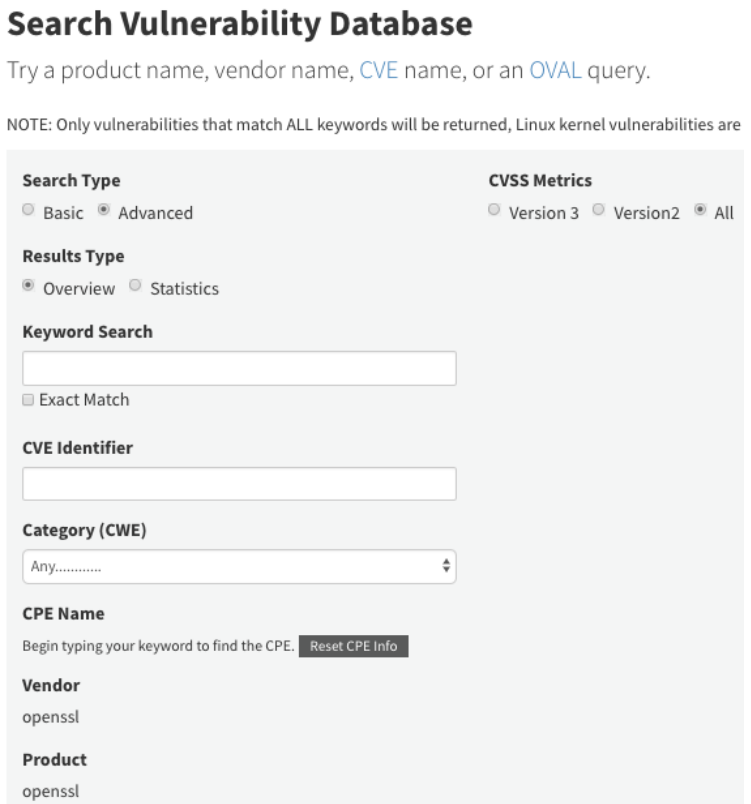
Product Name	Vendor Name	# Of CVE Entries	Product Type	OVAL Definitions			
				Vulnerabilities	Patches	Compliance	Inventory
Openssl	Openssl	187	Application	316	351	0	1

How do we keep Linux devices secure?

Manual process is expensive (1)

Software manifest

Name	Version
Linux kernel	4.4.15 LTS
openssl	1.0.2o
bash	4.4.19
...	...



Search Vulnerability Database

Try a product name, vendor name, CVE name, or an OVAL query.

NOTE: Only vulnerabilities that match ALL keywords will be returned, Linux kernel vulnerabilities are

Search Type
Basic Advanced

Results Type
Overview Statistics

Keyword Search
Exact Match

CVE Identifier

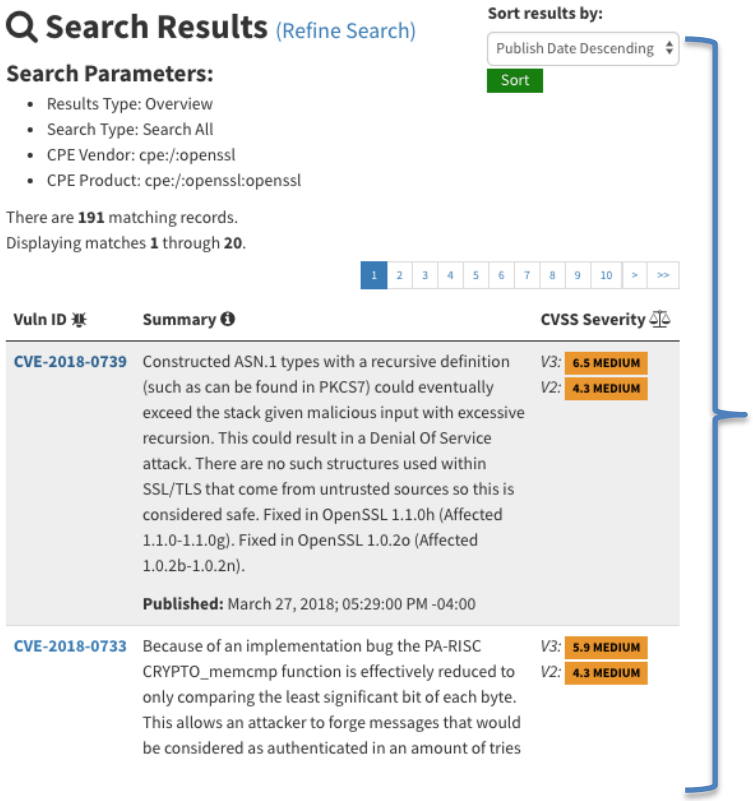
Category (CWE)
Any.....

CPE Name
Begin typing your keyword to find the CPE. Reset CPE Info

Vendor
openssl

Product
openssl

CVSS Metrics
Version 3 Version2 All



Search Results (Refine Search)

Sort results by: Publish Date Descending Sort

Search Parameters:
- Results Type: Overview
- Search Type: Search All
- CPE Vendor: cpe:/:openssl
- CPE Product: cpe:/:openssl:openssl

There are **191** matching records.
Displaying matches **1** through **20**.

1 2 3 4 5 6 7 8 9 10 > >>

Vuln ID	Summary	CVSS Severity
CVE-2018-0739	Constructed ASN.1 types with a recursive definition (such as can be found in PKCS7) could eventually exceed the stack given malicious input with excessive recursion. This could result in a Denial Of Service attack. There are no such structures used within SSL/TLS that come from untrusted sources so this is considered safe. Fixed in OpenSSL 1.1.0h (Affected 1.1.0-1.1.0g). Fixed in OpenSSL 1.0.2o (Affected 1.0.2b-1.0.2n). **Published:** March 27, 2018; 05:29:00 PM -04:00	V3: 6.5 MEDIUM V2: 4.3 MEDIUM
CVE-2018-0733	Because of an implementation bug the PA-RISC CRYPTO_memcmp function is effectively reduced to only comparing the least significant bit of each byte. This allows an attacker to forge messages that would be considered as authenticated in an amount of tries	V3: 5.9 MEDIUM V2: 4.3 MEDIUM

Challenges

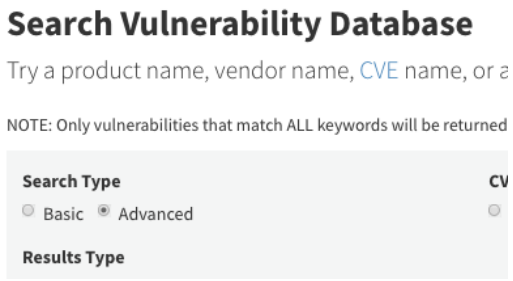
- Difficult to identify which open source are used/maintained
- There is no unified name for open sources. CVE can be reported for linux-kernel, linux, kernel, etc.

Manual process is expensive (2)

Upgrade

Find version

times no. of versions



Replaced Software

Patch

Find patch

times no. of CVEs

```
diff --git a/drivers/usb/core/hub.c b/drivers/usb/core/hub.c
index 0f38f57..6d84f6c 100644
--- a/drivers/usb/core/hub.c
+++ b/drivers/usb/core/hub.c
@@ -632,12 +632,17 @@ void usb_wakeup_notification(struct usb_device *hdev,
                unsigned int portnum)
 {
        struct usb_hub *hub;
+       struct usb_port *port_dev;

        if (!hdev)
                return;

        hub = usb_hub_to_struct_hub(hdev);
        if (hub) {
+               port_dev = hub->ports[portnum - 1];
+               if (port_dev && port_dev->child)
+                       pm_wakeup_event(&port_dev->child->dev, 0);
+
                set_bit(portnum, hub->wakeup_bits);
                kick_hub_wq(hub);
        }
@@ -3361,8 +3366,11 @@ int usb_port_resume(struct usb_device *udev, pm_message_t msg)

        /* Skip the initial Clear-Suspend step for a remote wakeup */
        status = hub_port_status(hub, port1, &portstatus, &portchange);
-       if (status == 0 && !port_is_suspended(hub, portstatus))
+       if (status == 0 && !port_is_suspended(hub, portstatus)) {
```

Fixed all CVEs

Release

Challenges

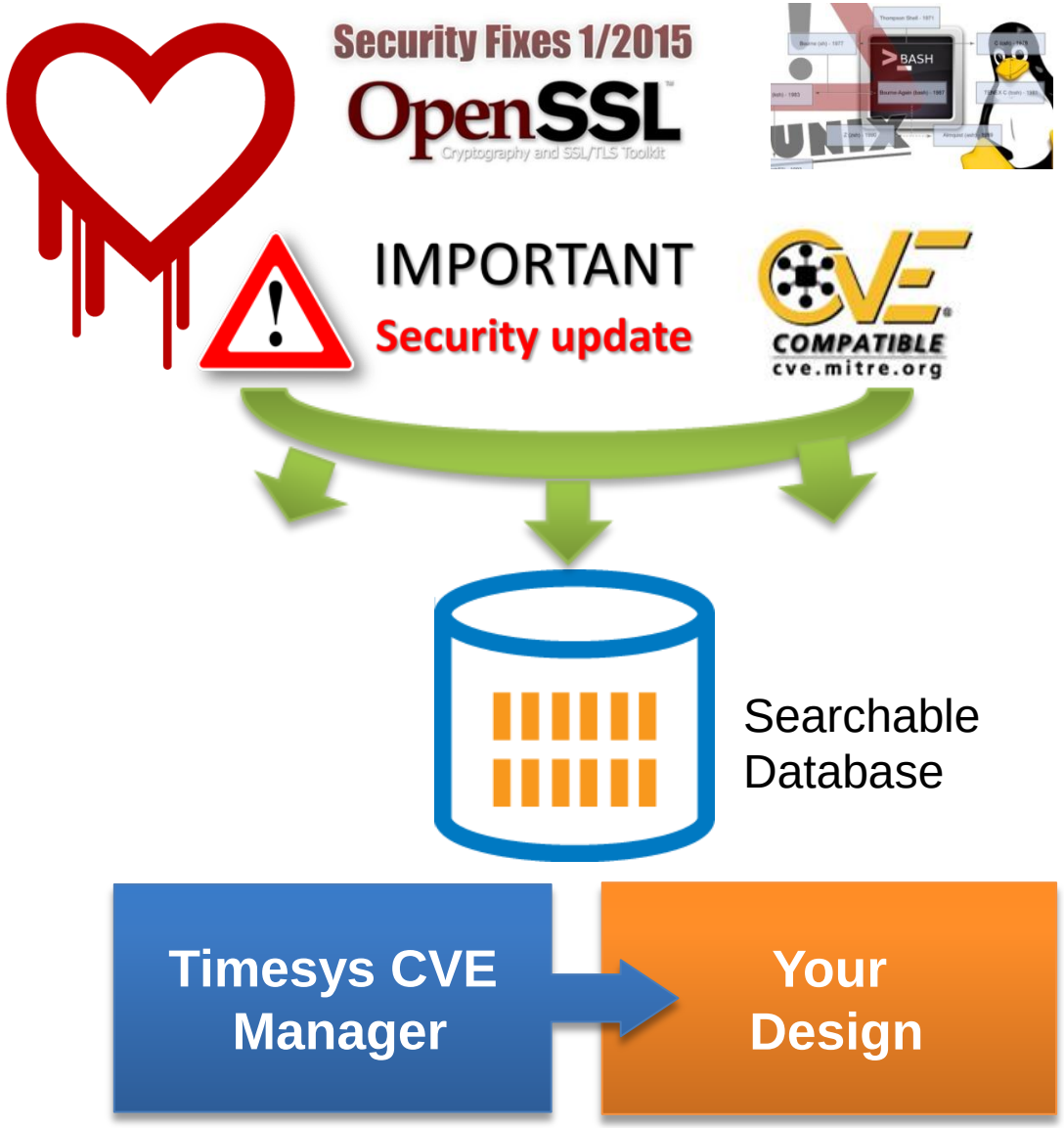
- Finding software versions that could be used and are maintained is very time consuming
- Difficult to find correct patches for all CVEs
- Replacing software in released products can be very invasive

Stay Secure

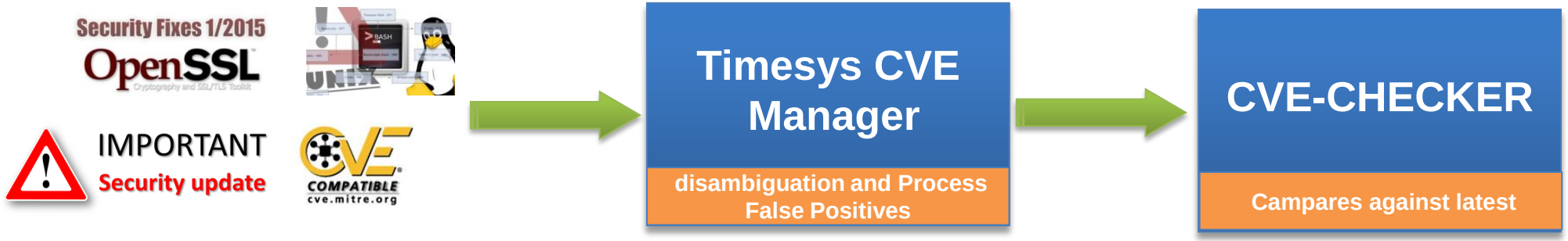
Solution for Security Vulnerability and Patch Notification

Security Notification Service

- **Common Vulnerabilities and Exposures (CVE) Manager**
  - Tracks security issues from multiple sources
- **Check against your specific software platform (manifest) and notify**
  - Always relevant
- **Differentiate between Unfixed and Fixed**

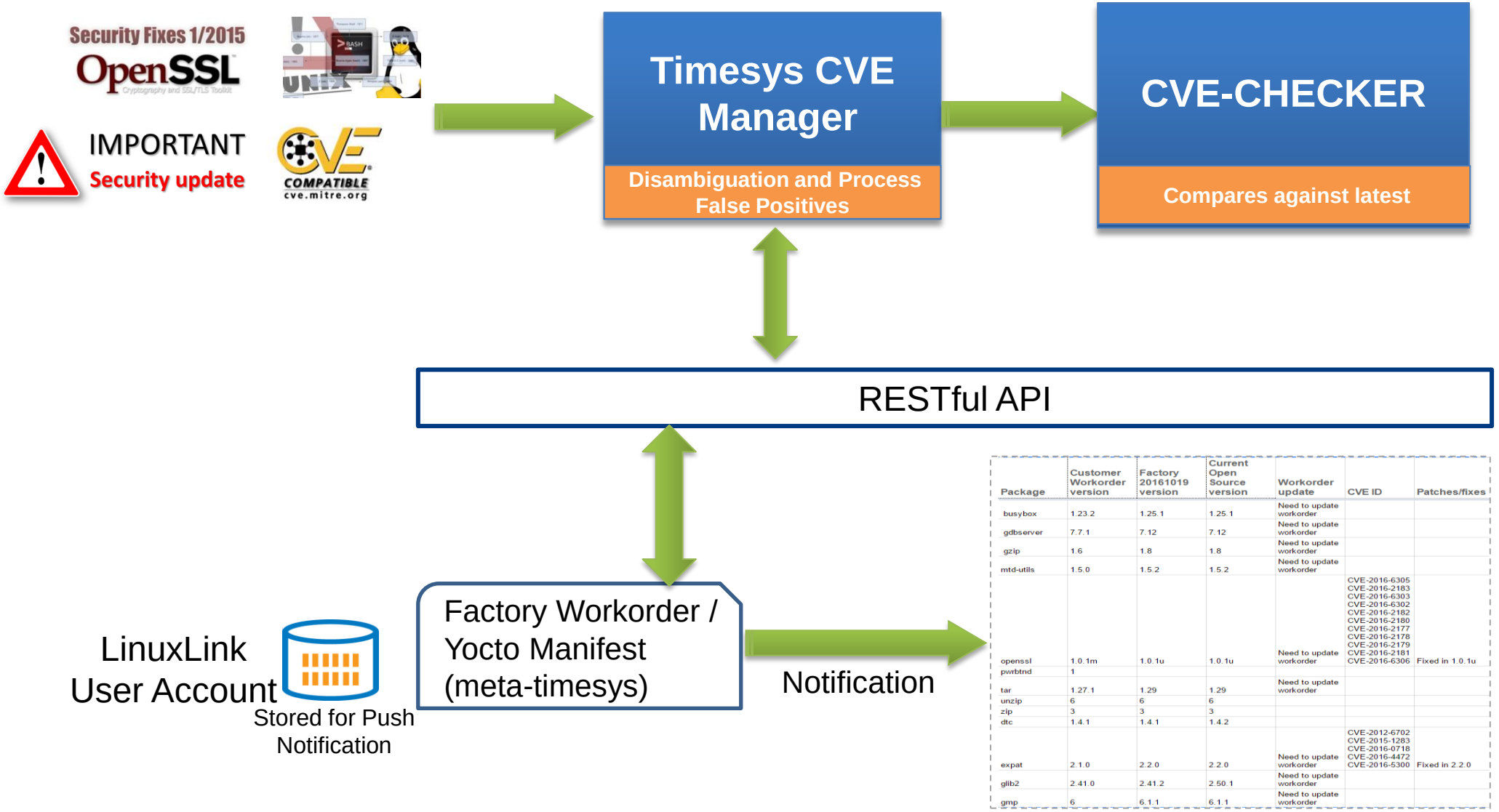


CVE Manager



- **Disambiguation**
  - Package names in the CVE database are not exactly the same as in the distributions (Differences between Factory,Yocto and upstream naming)
- **Only keep relevant**
  - Easy to discern by analyzing the summary
  - Filters out irrelevant CVEs (Oracle db, Windows)
- **False Positives**
  - Possibly relevant but has to be analyzed by an engineer in details
  - E.g. Searching Perl might bring up a CVE but the vulnerability is in a library/module used by the Perl script (marked as a false positive)

CVE Manager Notification (Push and Pull)



Package	Customer Workorder version	Factory 20161019 version	Current Open Source version	Workorder update	CVE ID	Patches/fixes
busybox	1.23.2	1.25.1	1.25.1	Need to update workorder		
gdbserver	7.7.1	7.12	7.12	Need to update workorder		
gzip	1.6	1.8	1.8	Need to update workorder		
mtd-utils	1.5.0	1.5.2	1.5.2	Need to update workorder		
openssl	1.0.1m	1.0.1u	1.0.1u	Need to update workorder	CVE-2016-6305 CVE-2016-2183 CVE-2016-6303 CVE-2016-6302 CVE-2016-2182 CVE-2016-2180 CVE-2016-2177 CVE-2016-2178 CVE-2016-2179 CVE-2016-2181 CVE-2016-6306	Fixed in 1.0.1u
pwrbtnd	1					
tar	1.27.1	1.29	1.29	Need to update workorder		
unzip	6	6	6			
zip	3	3	3			
dtc	1.4.1	1.4.1	1.4.2			
expat	2.1.0	2.2.0	2.2.0	Need to update workorder	CVE-2012-6702 CVE-2015-1283 CVE-2016-0718 CVE-2016-4472 CVE-2016-5300	Fixed in 2.2.0
glib2	2.41.0	2.41.2	2.50.1	Need to update workorder		
gmp	6	6.1.1	6.1.1	Need to update workorder		

Ongoing security

meta-timesys

- **Ongoing security for a product developed with Yocto Project is enabled via Timesys provided meta-timesys layer**
  - Works with any Bitbake based BSP build system
  - Uses secure communication with Timesys servers
  - Security provided on specific BSP image (configuration)
    - No security feed for package recipes present in Yocto but not used in the product
- **How to run it:**
  - Step 1: Setup bitbake run shell
  - Step 2: From within build directory run the following command:

```
$ ../layers/meta-timesys/scripts/manifest.sh fb-multimedia-full manifest.json
```

  - Step 3: Look at the report. Check for security issues

```
$ ../layers/meta-timesys/scripts/checkcves.py ./manifest.json
```

  - Step 4: Current security information displayed on your screen

Software manifest example


```
      "layer": "meta",
      "patched_cves": {},
      "version": "1.60.0"
    },
    "buildtools-tarball": {
      "branch": "HEAD",
      "layer": "meta",
      "patched_cves": {},
      "version": "1.0"
    },
    "busybox": {
      "branch": "HEAD",
      "layer": "meta",
      "patched_cves": {
        "CVE-2016-2147": [
          "/home/tsu/LAB-Advantech/imx6LBV8090_rsb4411a1/sources/poky/meta/recipes-core/busybox/busybox/
CVE-2016-2147.patch",
          "/home/tsu/LAB-Advantech/imx6LBV8090_rsb4411a1/sources/poky/meta/recipes-core/busybox/busybox/
CVE-2016-2147_2.patch"
        ],
        "CVE-2016-2148": [
          "/home/tsu/LAB-Advantech/imx6LBV8090_rsb4411a1/sources/poky/meta/recipes-core/busybox/busybox/
CVE-2016-2148.patch"
        ]
      },
      "version": "1.24.1"
    },
    "bzip2": {
      "branch": "HEAD",
                                                                                    211,1          14%
```

Vulnerability Pull Notification — cvecheck

```
Recipe:  dosfstools
Version: 3.0.28
CVE ID:  CVE-2015-8872
URL:     https://nvd.nist.gov/vuln/detail/CVE-2015-8872
CVSSv2:  2.1
Vector:  LOCAL
Status:  Unfixed

Recipe:  dpkg
Version: 1.18.4
CVE ID:  CVE-2017-8283
URL:     https://nvd.nist.gov/vuln/detail/CVE-2017-8283
CVSSv2:  7.5
Vector:  NETWORK
Status:  Unfixed

Recipe:  expat
Version: 2.1.0
CVE ID:  CVE-2015-1283
URL:     https://nvd.nist.gov/vuln/detail/CVE-2015-1283
CVSSv2:  6.8
Vector:  NETWORK
Status:  Fixed
Patched by:
         /home/tsu/LAB-Advantech/imx6LBV8090_rsb4411a1/sources/poky/meta/recipes-core/expat/expat-2.1.0/e
xpat-CVE-2015-1283.patch
```

Vulnerability Notification — On Demand Report

LinuxLink by timesys | Search LinuxLink | Timesys Only | Support | Docs | Resources | Git Repos | Security | Tools | Maciej

CVE Report

Image: fsl-image-multimedia-full

Machine: imx6qrsb4411a1

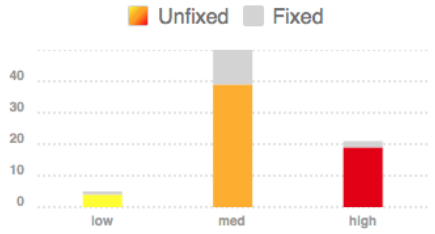
Distro: master (4.1.15-2.1.0)

Generated: 05/16/18 04:49 PM UTC

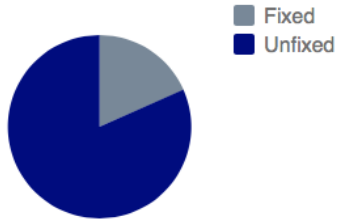
NOTE: Rows highlighted in red have a high CVSSv2 score.

Summary

62	Unfixed
14	Fixed
0	CPU / Architecture
21	High CVSS



CVE Count by CVSS Range



CVE Count by Status

Unfixed CVEs 62

These are CVEs that affect the listed packages at the given version.

Package	Version	CVE ID	CVSSv2	Vector
avahi	0.6.32	CVE-2017-6519	6.4	NETWORK
busybox	1.24.1	CVE-2016-6301	7.8	NETWORK

Fixed CVEs 14

These CVEs are relevant to the corresponding package and version, but a patch is already applied to address them in your configuration.

Package	Version	CVE ID	CVSSv2	Vector
expat	2.1.0	CVE-2015-1283	6.8	NETWORK
libvorbis	1.3.5	CVE-2017-11333	4.3	NETWORK
libvorbis	1.3.5	CVE-2017-14632	7.5	NETWORK

ADVANTECH

Vulnerability — Push Notification

Search LinuxLink | Timesys Only | Support | Docs | Resources | Git Repos | Security | Tools | Maciej

Security Notification Management

Manage security notifications for your builds and view CVE Reports

NOTE: Click *new* in any row to generate a CVE report for that configuration now.

Update Subscriptions | Upload Config

Subscribed	Build Engine	Engine Version	Machine / Board	Image (Yocto only)	Date Submitted	CVE Reports	Delete
☑	Yocto	master 4.1.15-2.1.0	imx6qrsb4411a1	fsl-image-multimedia-full	05/16/18	latest – all – new	✕
☐	Yocto	master 4.1.15-2.1.0	imx6qrsb4411a1	fsl-image-multimedia-full	05/16/18	latest – all – new	✕

Stay Secure — patching

- **Patching – method of modifying source code by applying source patches (inserting/removing code)**
- **Manual process of patching security issues is quite complex**
  1. Identify patches that can be applied to a product configuration
     - Many sources
     - Need to analyze commit logs and issue reports
     - Monitor mailing lists
  2. Apply the patches in identified order
     - Update Yocto recipes
     - Decide if back-porting is needed
     - Test/Regression
  3. Maintain patches for the product lifetime
     - Manage package upgrades
     - Resolve patch conflicts
     - Monitor/Analyze updates to patches

- **Timesys provides an easy solution to the patching challenge**

Stay Secure — patching

meta-timesys-security

- **Solutions for both Yocto Project and Factory build systems**
- **Taking advantage of the solution is simple**

Download meta-timesys-security → Add Timesys solution to your Yocto Project (bblayers.conf) → Automatically receive/apply product relevant patches

- **Leverage Timesys TRST team work in your products**
  - No need to rely on active patch searches
  - No need to figure out if patch can be applied to product configuration
  - No need to use own resources to maintain security patches
  - Product engineering teams have ability to whitelist/blacklist patches

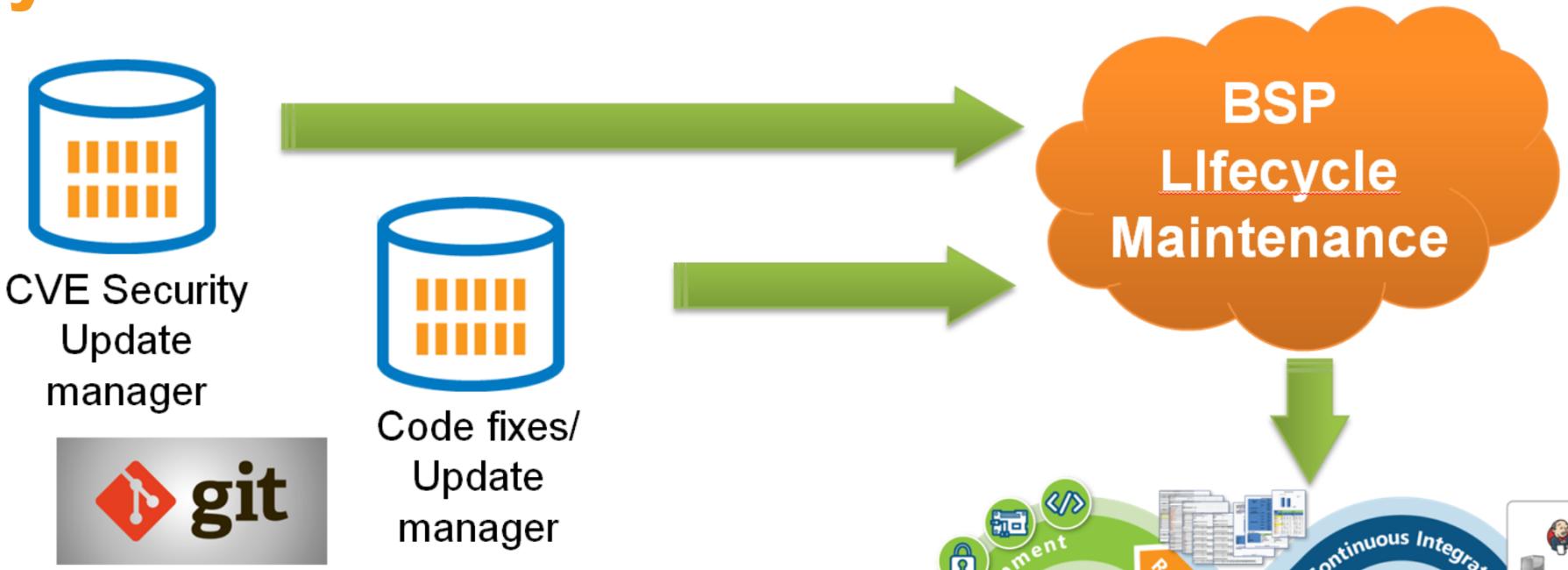
LAB
Ongoing Security

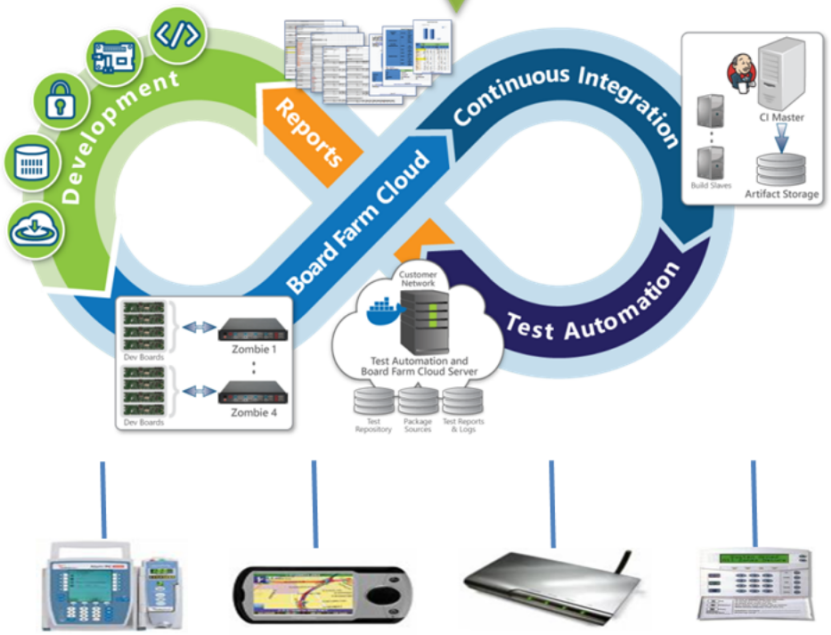
Timesys Security Vulnerability Notification Helps You Reduce Time and Cost

- **No work for you.** Because the TRST team maintains the Timesys CVE manager database for you, the amount of time spent having to monitor CVEs yourself is eliminated.
- **Filter out the noise.** You receive notification of vulnerabilities relevant to only your open source software, which means less information you need to sort through.
- **Get notification when you want it.** You decide how you want to receive notification, enabling you to get it when you need it.
- **Access CVE details easily.** Whether via command-line or web, you can access detailed information about a known CVE via the direct links provided.
- **Always know what is affected.** Can subscribe to Notification for each and every build.
- **Track changes conveniently.** The report history for all configurations is available in one place, making it quick and easy to see what's changed – newly discovered CVEs and fixed CVEs.

Assisting with maintenance of your Linux product

BSP Lifecyle Maintenance





- Offload the burden of maintaining the BSP
- Keep up with the asynchronous release schedule of the various components (compilers, user-space packages and kernel)
- Keep up with the security updates
- Provides Updated BSP and Test Reports

Timesys Security Offering Summary

Security Notification Subscription

Continuous Monitoring
Common Vulnerabilities
& Exposures (CVE)

Notification
Push and Pull

Stay Secure Service

Patching
BSP Lifecycle Maintenance

Deployment
High Assurance Boot

Secure By Design Service

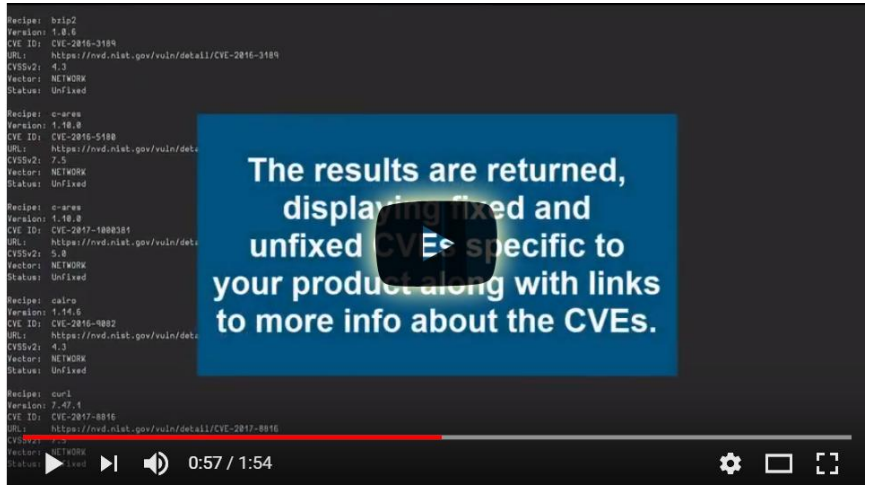
Security Audit and Scanning

Security Hardening

Security is an ongoing process and is not fool-proof. Timesys' security offering provides assistance with minimizing known vulnerabilities based on known issues, but doesn't provide any warranty.

Session takeaways

- **Stay Secure solution from Timesys solves ongoing security challenge for a product. *To view the complete Timesys Security Solution, visit www.timesys.com/security***
- **Download meta-timesys from https://www.github.com/TimesysGIT/meta-timesys**
  - Generate your manifest
- **Login to https://linuxlink.timesys.com and upload your manifest for immediate feedback on security vulnerability**
- **Watch a video at https://youtu.be/YHrFUKgm3yE**
- **Get a complimentary 90-day subscription to Timesys' Security Vulnerability Notification Service with select Advantech RISC platforms https://www.timesys.com/advantech**



Contact Us

North America Offices

(Corporate Headquarters)

1905 Boulevard of the Allies
Pittsburgh, PA 15219
UNITED STATES
T: +1.412.232.3250
Toll-free: 1.866.392.4897
sales@timesys.com

8153 Elk Grove Boulevard
Suite 20
Elk Grove, CA 95758-5965
UNITED STATES
T: +1.916.753.9351
Toll-free: 1.866.392.4897
sales@timesys.com

EMEA Office

Ul Palmowa 1A
62-081 Chyby, POLAND
T: +48.53.733.8080
emea@timesys.com

Request a personalized, live demo and/or quote.

APAC Offices

3rd Floor, Time Square Building,
Shushant Marg, Sushant Lok I,
Sector 43, Gurugram,
Haryana – 122015, INDIA
apac@timesys.com

3rd Floor
Jaag Homes, Achyutha Square, No. 3,
MTH Road, Villivakkam, Chennai,
Tamil Nadu – 600 050, INDIA
apac@timesys.com

1st Floor
31/1, Old Damu Nagar,
Puliyakulam, Coimbatore,
Tamil Nadu – 641 045, INDIA
apac@timesys.com

Technical Support

https://linuxlink.timesys.com/support