BSP SECURITY MAINTENANCE

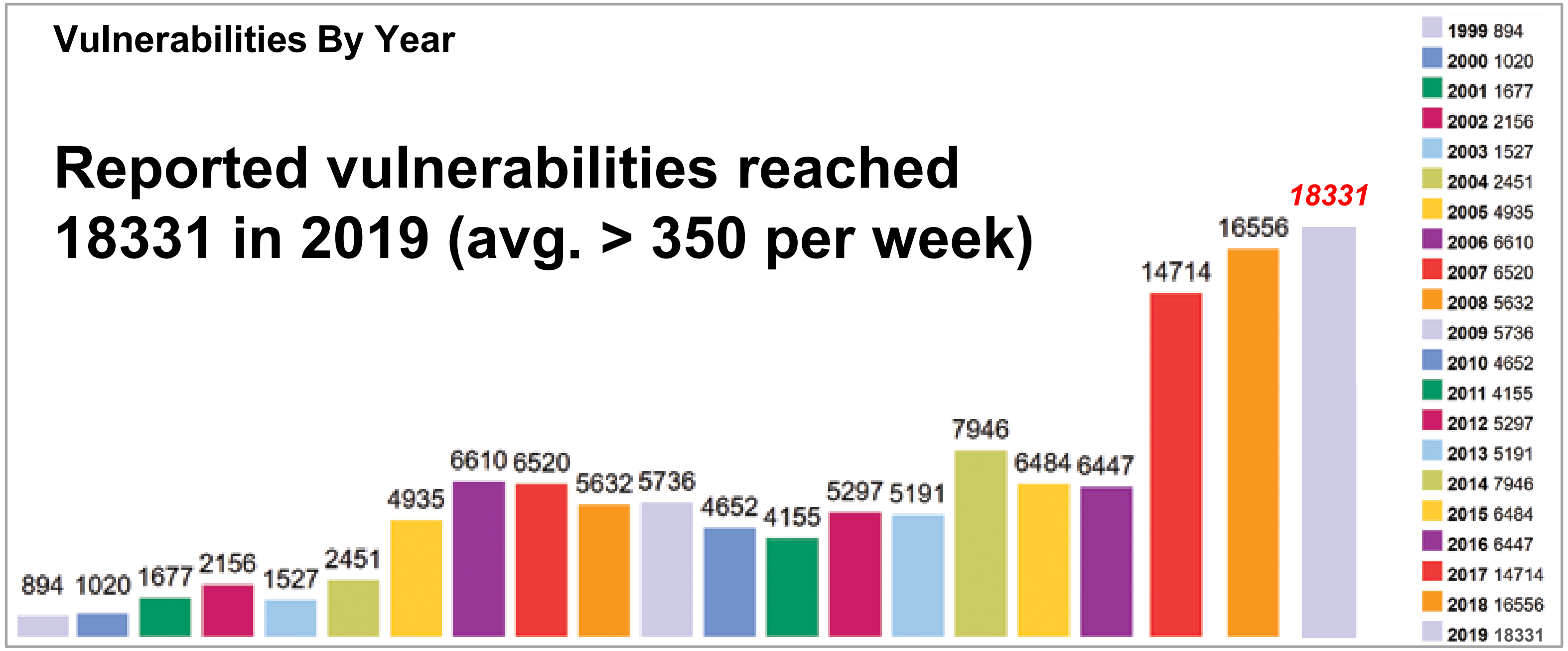
Best practices for vulnerability monitoring and remediation

April 2020

NXP External Use

SECURE CONNECTIONS
FOR A SMARTER WORLD

Managing the growing tsunami of new vulnerabilities



Vulnerabilities By Year

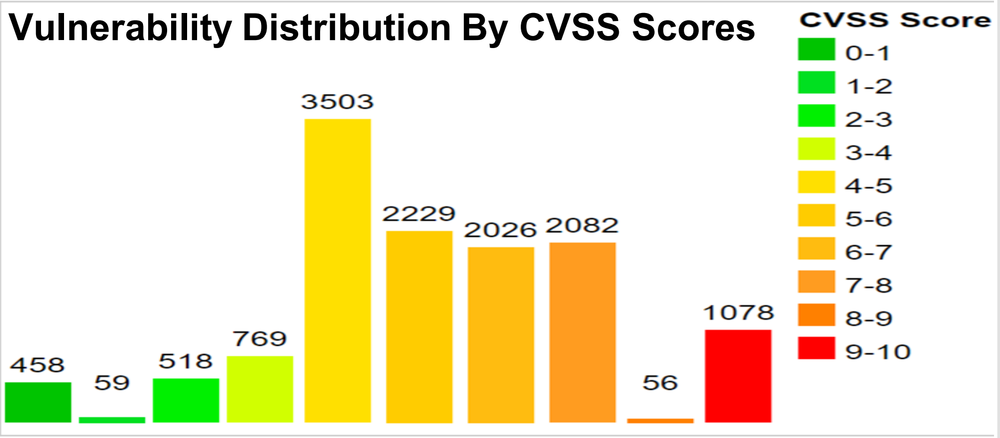
Reported vulnerabilities reached 18331 in 2019 (avg. > 350 per week)

- **An endless cycle or a balancing act?**
  1. Maintain development schedules
  2. Regular monitoring for new vulnerabilities
  3. Minimize the resource overhead

This flow must be a manageable, repeatable process or it will be overwhelming

Issue severity scores

(all issues) **Avg. = 6.1**

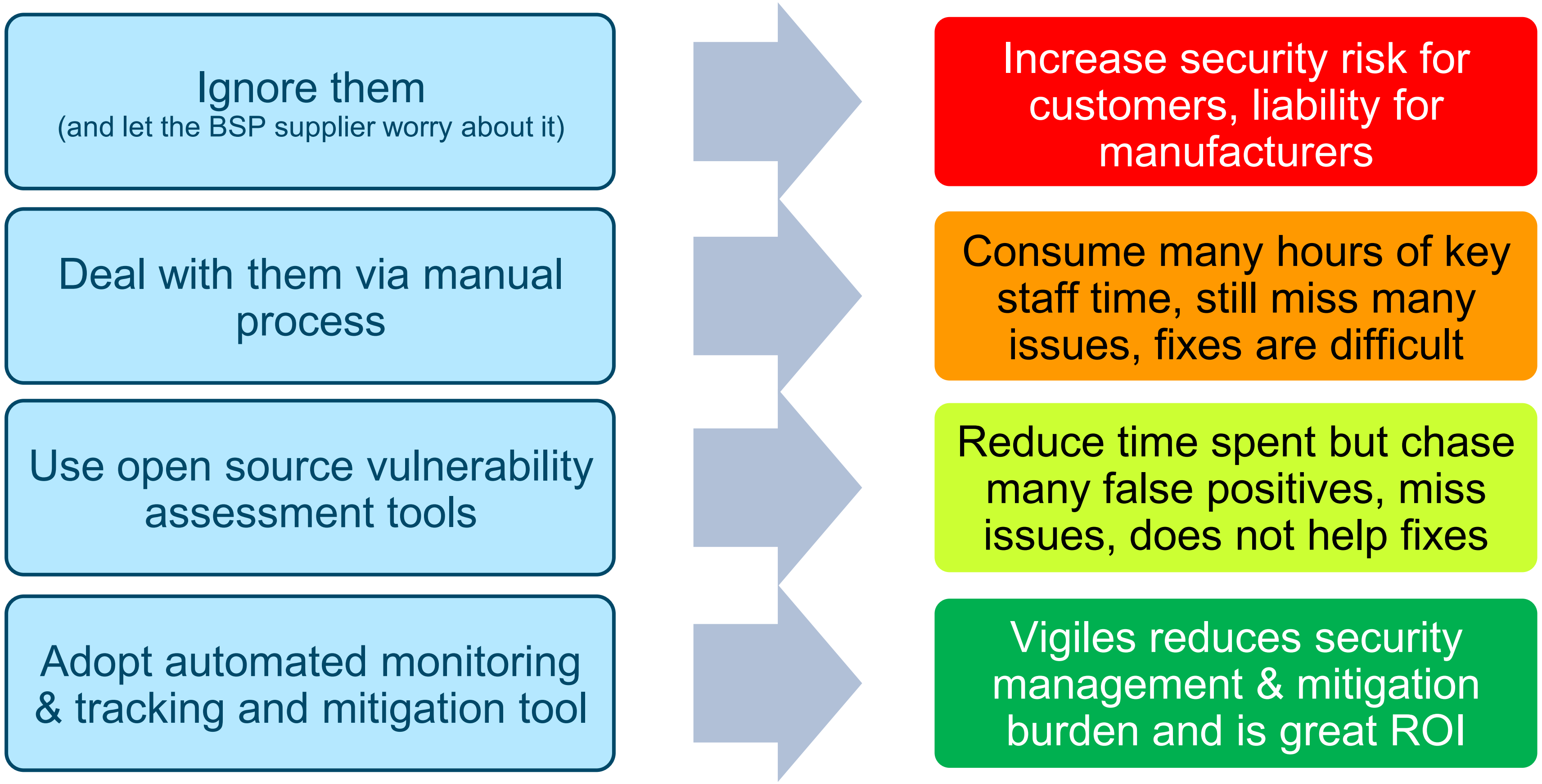


Vulnerability Distribution By CVSS Scores

Source: cvedetails

Options for dealing with outstanding CVEs

With 350+ vulnerabilities reported each week, product developers can choose to …



Ignore them
(and let the BSP supplier worry about it)

Increase security risk for customers, liability for manufacturers

Deal with them via manual process

Consume many hours of key staff time, still miss many issues, fixes are difficult

Use open source vulnerability assessment tools

Reduce time spent but chase many false positives, miss issues, does not help fixes

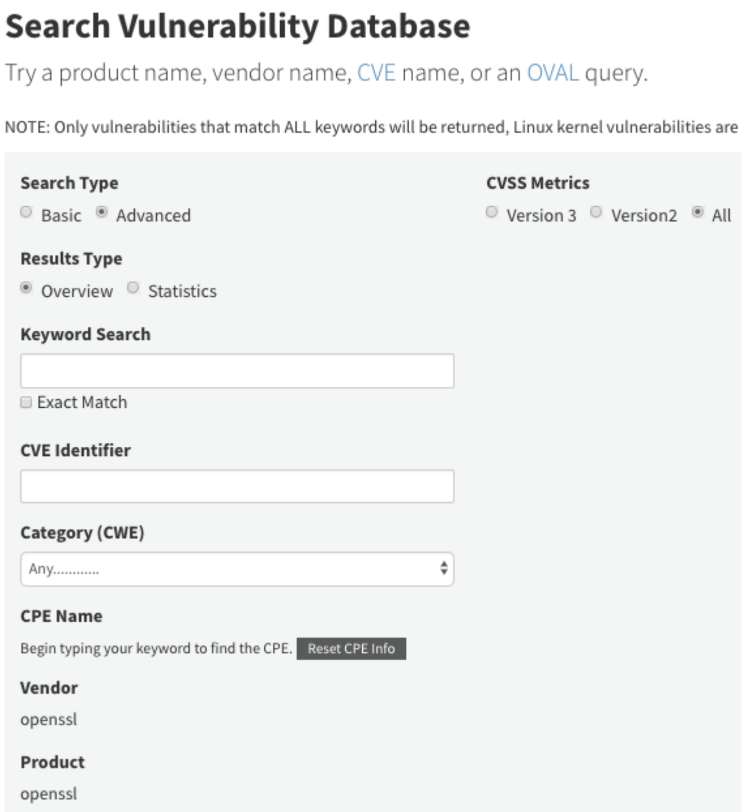
Adopt automated monitoring & tracking and mitigation tool

Vigiles reduces security management & mitigation burden and is great ROI

Manual monitoring process is expensive and error-prone

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

CVSS Metrics

○ Version 3 ○ Version2 ● All

Results Type

● Overview ○ Statistics

Keyword Search

□ Exact Match

CVE Identifier

Category (CWE)

Any...........

CPE Name

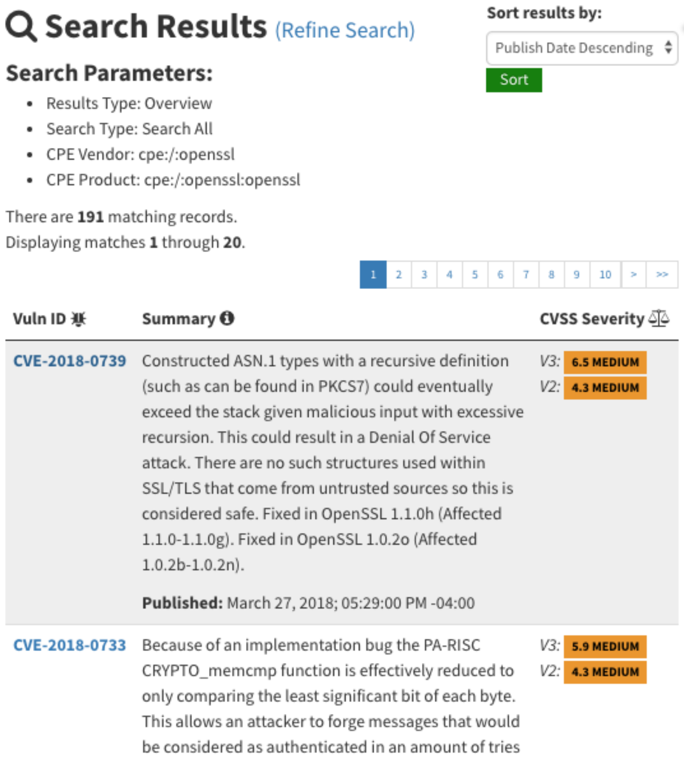
Begin typing your keyword to find the CPE. Reset CPE Info

Vendor

openssl

Product

openssl



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**.

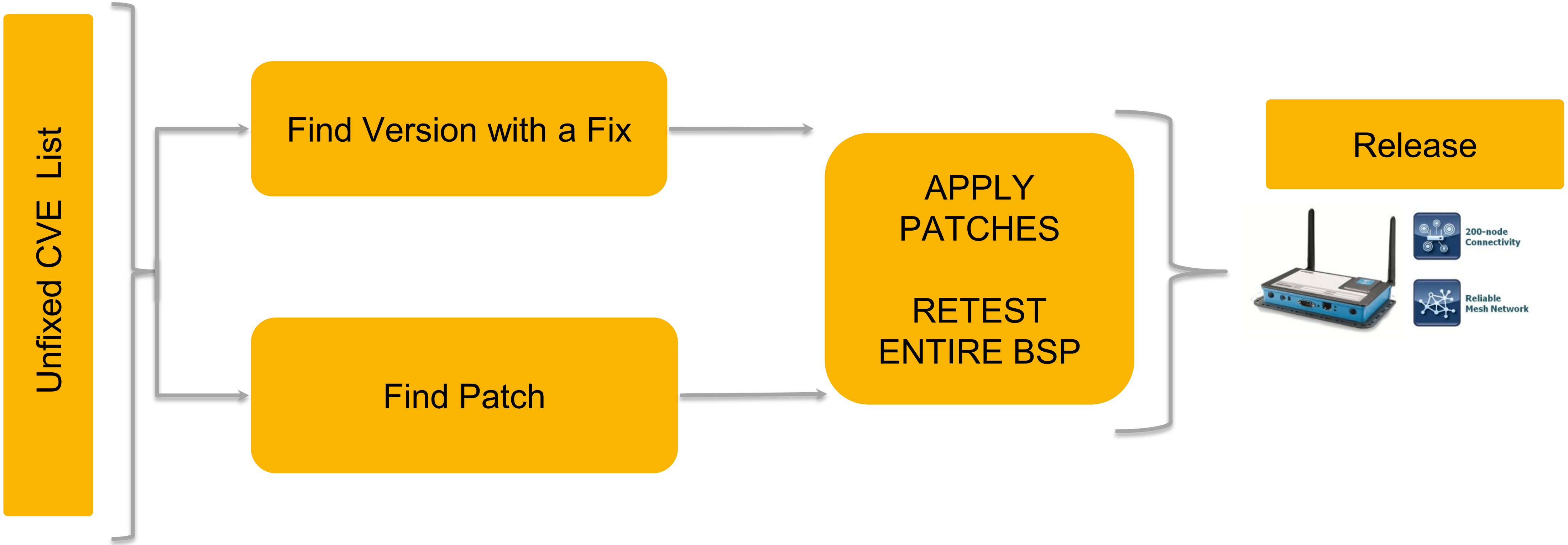
1 2 3 4 5 6 7 8 9 10 > >>

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 of finding & analyzing patches is time-consuming



Unfixed CVE List

Find Version with a Fix

Find Patch

APPLY PATCHES

RETEST ENTIRE BSP

Release

Challenges

- Finding software versions that could be used and are maintained is very time-consuming

- Difficult to find correct patches for all CVEs

- Testing patches
- Retesting entire BSP

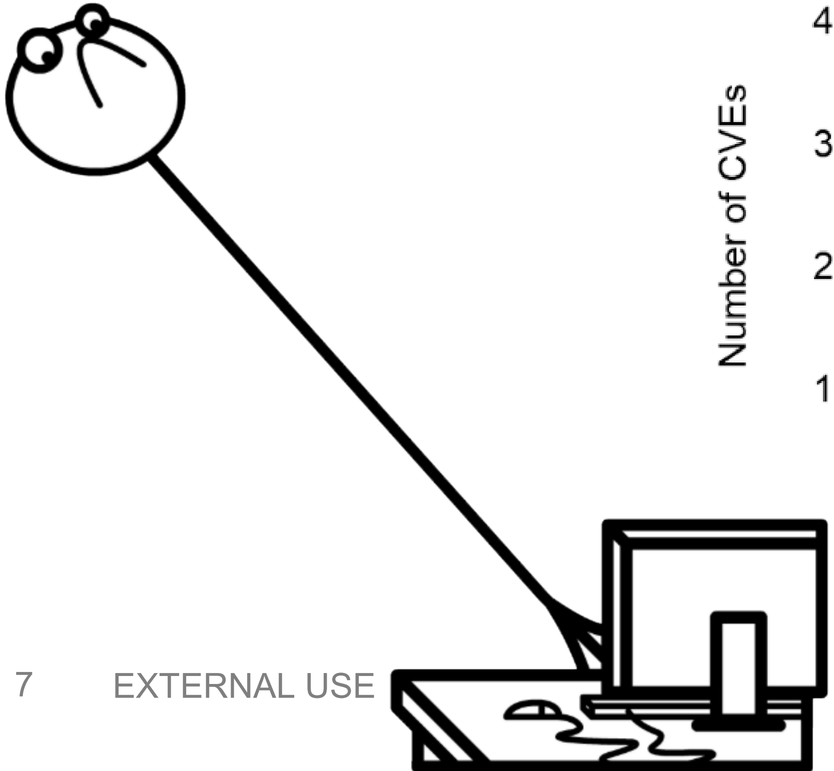
Challenges with keeping devices secure – CVE data quality

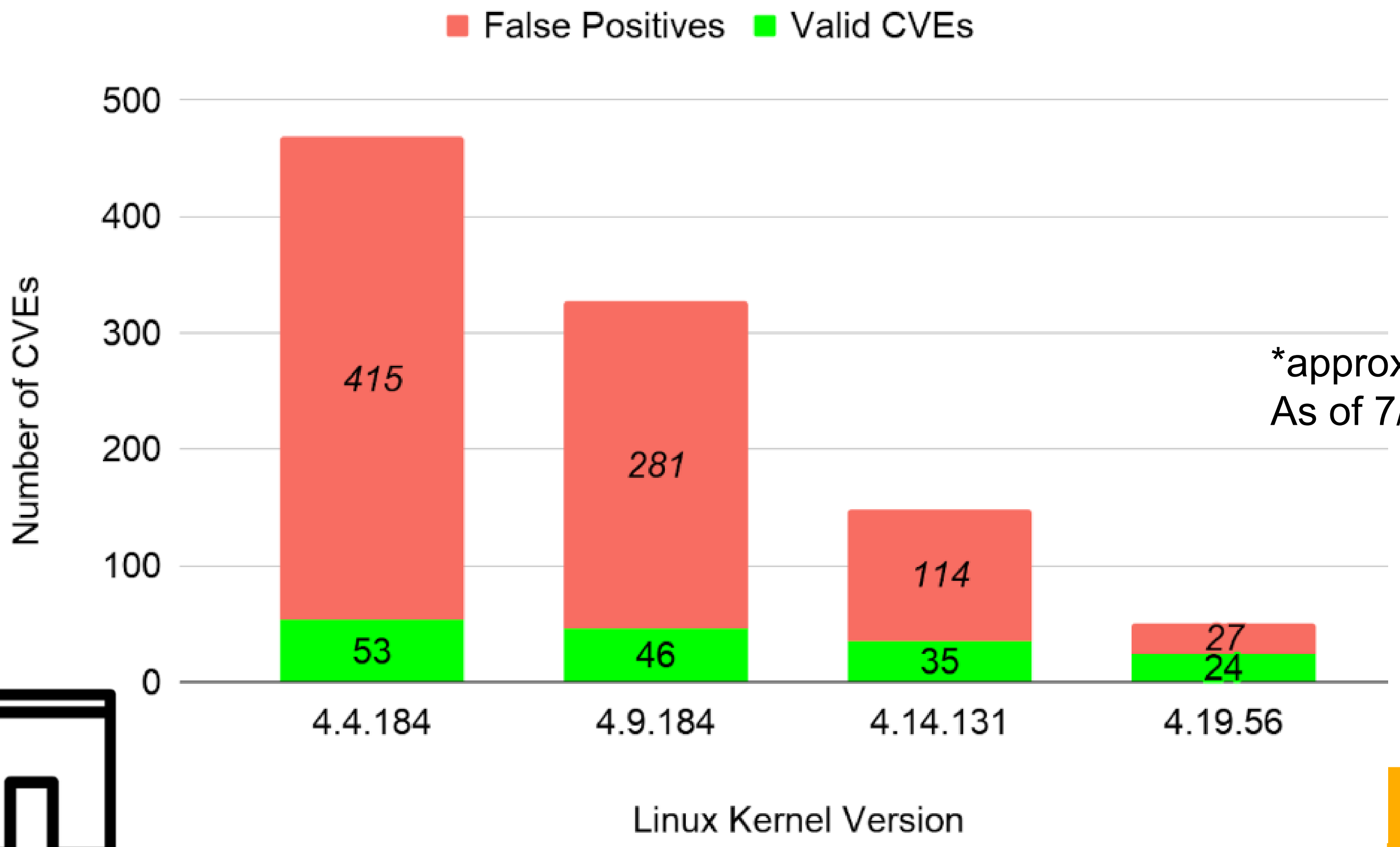
(False positives and misses)

- Inconsistent naming
  - arm-trusted-firmware, arm_trusted_firmware, trusted_firmware-a
- Typos
  - Version number
    - CVE-2016-1234: 2.2.3 instead of 2.23 (corrected now)
  - CVE product name
    - CVE-2016-1494: python instead of rsa (corrected now)
- Incorrect/incomplete analysis
  - CVE-2018-14618: up to 7.61.1 instead of 7.15.4 to 7.61.1
- Outdated information
  - Kernel CVEs (more later)
- No version or cpe information
  - CVE-2018-10845: cpe:2.3:a:gnu:gnutls:-:*:*:*:*:*:*:*

Challenges with keeping devices secure – Linux kernel CVEs

- Typically, new CVE is listed as affecting all versions till latest
- Kernel maintainers do a fantastic job at backporting fixes to LTS
  - NVD CPE info not updated when patches backported





*approx numbers:
As of 7/30/2019

Challenges with keeping devices secure – delays in CVE reporting / analysis

CVE-2019-6690 (python-gnupg)

1/19: Vulnerability discovered (private)

1/20: PoC created

1/22: Applied for CVE, vendor notified

1/23: CVE-2019-6690 assigned

1/23: Vendor responded, fix committed

1/25: Disclosed on oss-security (public)

3/21: NVD publishes CVE

4/2 : NVD analysis - adds cpe tags

68 days from being public to NVD analysis

CVE-2019-5436 (libcurl)

4/29: Reported on hackerone (private)

4/29: Fix developed (private)

5/15: Disclosed on distros list (private)

5/20: Fix appears on github

5/22: Disclosed on oss-security (public)

5/28: NVD publishes CVE

5/29: NVD analysis - adds cpe tags

7 days from being public to NVD analysis

NXP Presents Vigiles*: Keeping your Linux BSP Secure

www.nxp.com/vigiles

Staying secure is a process that must be implemented by every engineering team

- ***BSPs*** become an aging snapshot as soon as they are released.
  - Recently, ***over 350 new CVEs are reported weekly***, resulting in possible exposure to new ***security issues*** every week!
  - While customers spend an additional 6, 9 or 12+ months developing the final product, ***thousands of CVE's*** have been reported.

- ***Vigiles*** enables development teams to quickly and efficiently analyze reported issues and ***take action***
  - Automatically ***scans*** for ***and identifies vulnerabilities*** specific to your projects and software components
  - Produces ***highly accurate vulnerability reports***, which combined with a very low false positive rate, provides ongoing software security maintenance that is streamlined, repeatable and highly efficient
  - ***Identifies available patches***, even if they are released on a newer version!

VIGILES™

Features

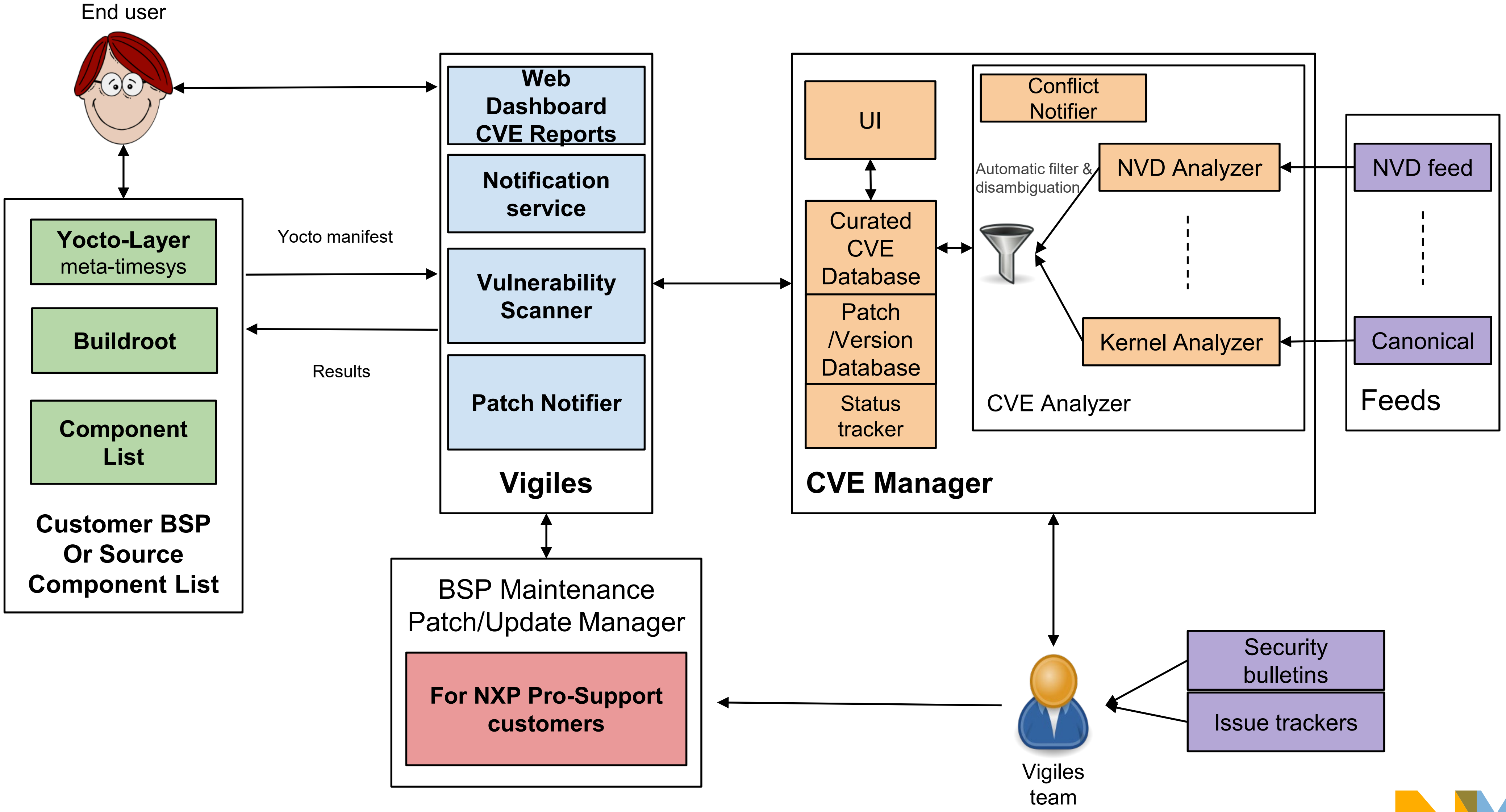
- On-demand vulnerability reports
- Automatic alerts for newly discovered CVEs
- Filtering CVEs by severity and whitelisting non-issues
- Provides direct link to fixes
- Can be bundled with Pro-Support for assistance

Benefits

- Maintain strong product security throughout your product lifecycles
- Bring more secure products to market faster
- Make security a key product differentiator
- Works with ANY Yocto based BSP
- **Start for free**

** Vigiles is powered by a Timesys*

Vigiles Technology Architecture



NXP Yocto – Vigiles starting point

- Vigiles is enabled with a Yocto metalayer (meta-timesys)
- Easily used with NXP Yocto Project
  - Can be added to any NXP Yocto BSP (https://github.com/TimesysGit/meta-timesys)

```
RELEASE=thud
git clone https://github.com/TimesysGit/meta-timesys.git -b $RELEASE
```

  - Comes pre-integrated into NXP's Yocto BSP - starting from Yocto "Thud" (https://source.codeaurora.org/external/imx/imx-manifest/)

Vigiles process for Yocto Project

- Step 1: Configure your Yocto build for scanning with Vigiles (in conf/local.conf)

```
INHERIT += "vigiles"
VIGILES_KEY_FILE = "/tools/timesys/linuxlink_key"
```

- Step 2: Fine tune the scanning results by pointing to your Linux kernel configuration

```
VIGILES_KERNEL_CONFIG = "/projects/kernel/linux-4.14-ts+imx-1.0/.config"
```

- Step 3: Run the scan

```
$ bitbake -c vigiles_check core-image-minimal
```

- Step 4: Look at the report locally
- Step 5: Look at the details, analyze, and triage using Vigiles online UI

Vigiles Process Walkthrough

Vigiles Scan Tool

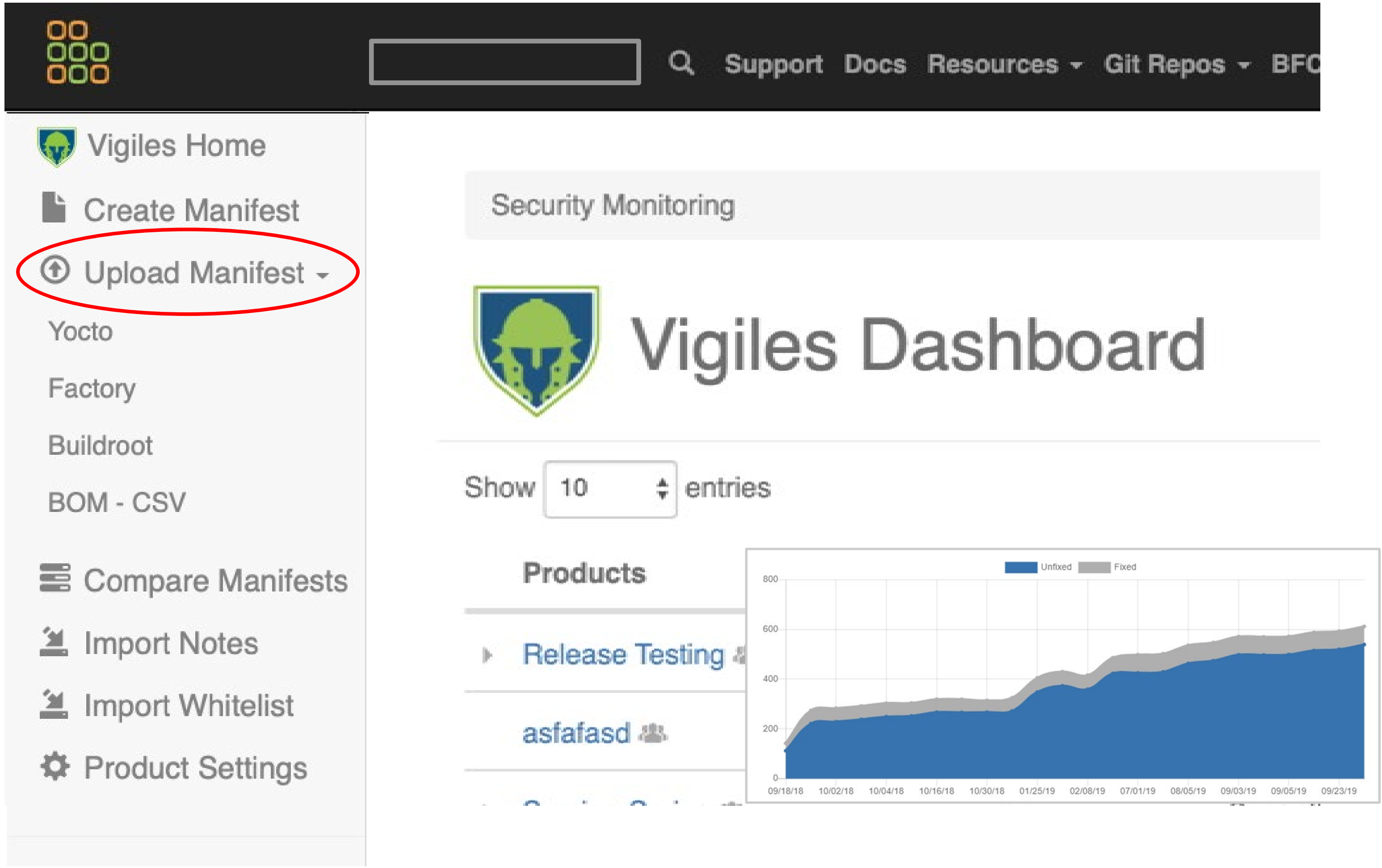
Upload Yocto, Buildroot, Factory, or CSV manifests

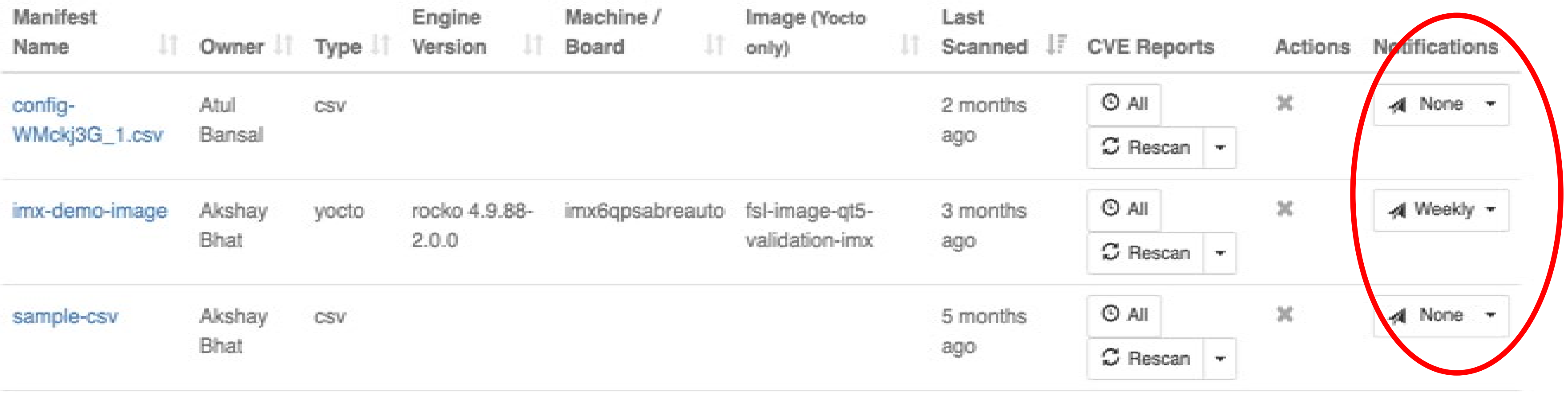
Yocto – Command-line Capable

Team Sharing for Triage Collaboration

Notification Management

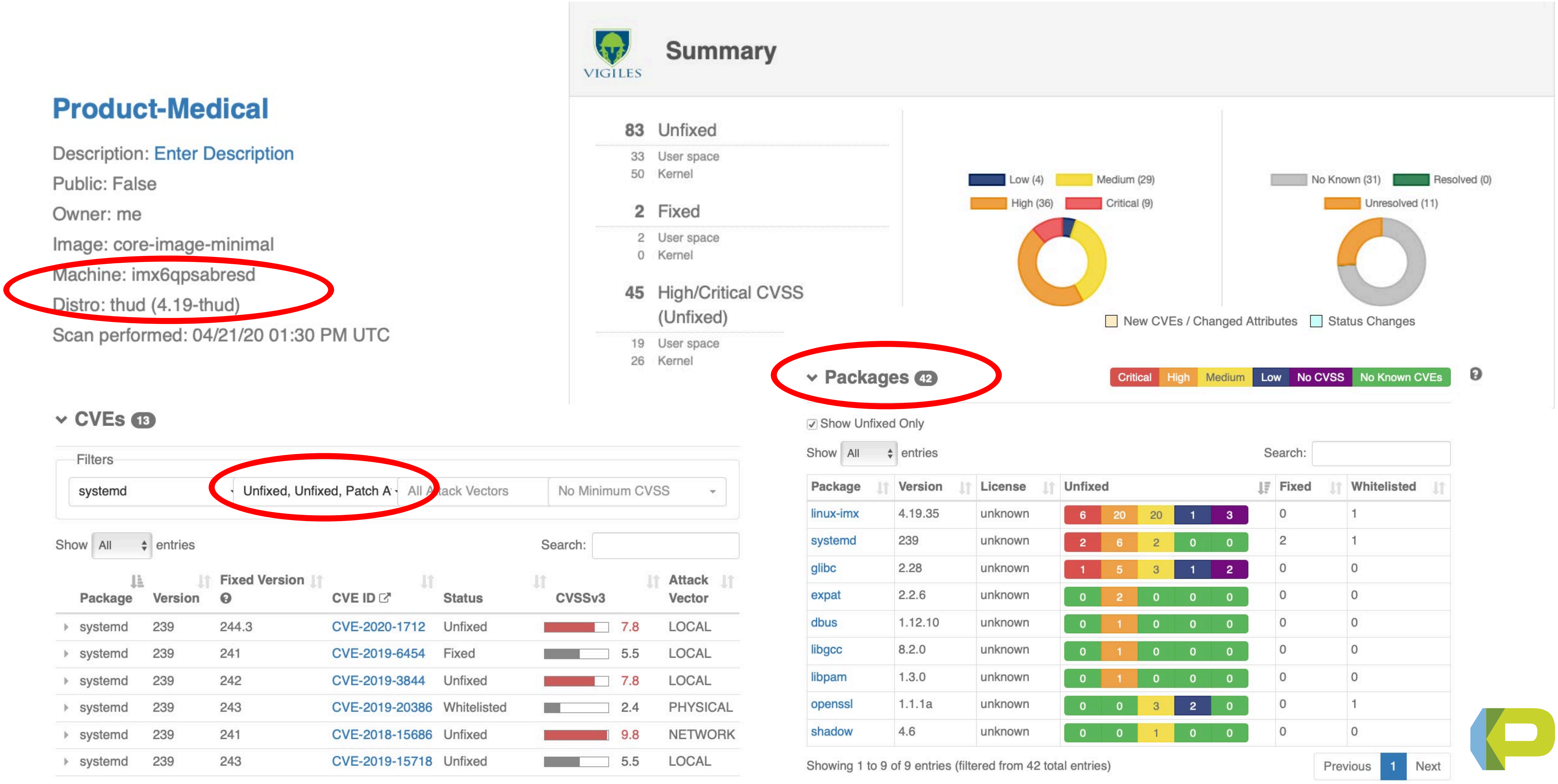
Unfixed and Fixed CVE Trend





Manifest Name	Owner	Type	Engine Version	Machine / Board	Image (Yocto only)	Last Scanned	CVE Reports	Actions	Notifications
config-WMckj3G_1.csv	Atul Bansal	csv				2 months ago	All Rescan	✖	None
imx-demo-image	Akshay Bhat	yocto	rocko 4.9.88-2.0.0	imx6qpsabreauto	fsl-image-qt5-validation-imx	3 months ago	All Rescan	✖	Weekly
sample-csv	Akshay Bhat	csv				5 months ago	All Rescan	✖	None

Vigiles: BASIC – On-Demand Report



Product-Medical

Description: Enter Description

Public: False

Owner: me

Image: core-image-minimal

Machine: imx6qpsabresd

Distro: thud (4.19-thud)

Scan performed: 04/21/20 01:30 PM UTC

VIGILES

Summary

83	Unfixed
33	User space
50	Kernel
2	Fixed
2	User space
0	Kernel
45	High/Critical CVSS (Unfixed)
19	User space
26	Kernel

□ New CVEs / Changed Attributes □ Status Changes

CVEs 13

Filters

systemd | Unfixed, Unfixed, Patch A | All Attack Vectors | No Minimum CVSS

Show All entries Search:

Package	Version	Fixed Version ❓	CVE ID	Status	CVSSv3	Attack Vector
systemd	239	244.3	CVE-2020-1712	Unfixed	7.8	LOCAL
systemd	239	241	CVE-2019-6454	Fixed	5.5	LOCAL
systemd	239	242	CVE-2019-3844	Unfixed	7.8	LOCAL
systemd	239	243	CVE-2019-20386	Whitelisted	2.4	PHYSICAL
systemd	239	241	CVE-2018-15686	Unfixed	9.8	NETWORK
systemd	239	243	CVE-2019-15718	Unfixed	5.5	LOCAL

Packages 42

Critical | High | Medium | Low | No CVSS | No Known CVEs

☑ Show Unfixed Only

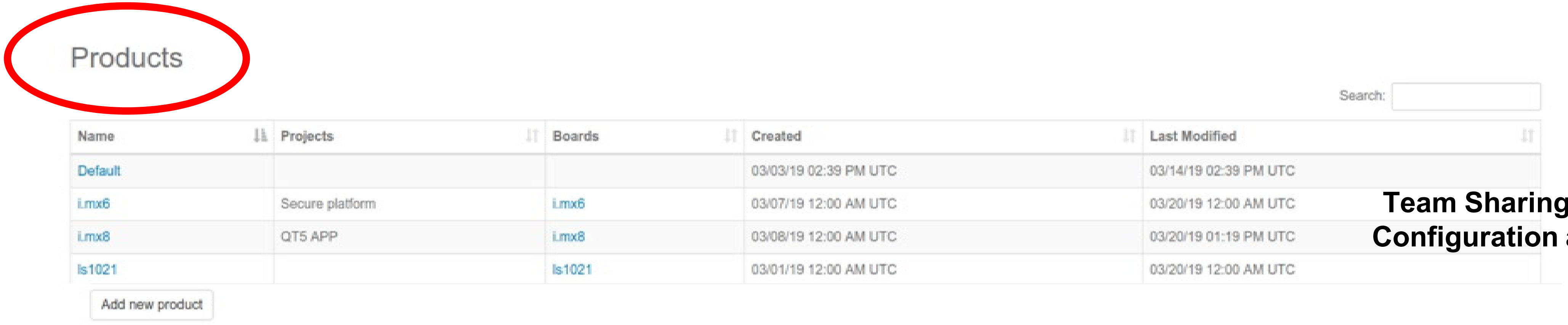
Show All entries Search:

Package	Version	License	Unfixed	Fixed	Whitelisted
linux-imx	4.19.35	unknown	6 20 20 1 3	0	1
systemd	239	unknown	2 6 2 0 0	2	1
glibc	2.28	unknown	1 5 3 1 2	0	0
expat	2.2.6	unknown	0 2 0 0 0	0	0
dbus	1.12.10	unknown	0 1 0 0 0	0	0
libgcc	8.2.0	unknown	0 1 0 0 0	0	0
libpam	1.3.0	unknown	0 1 0 0 0	0	0
openssl	1.1.1a	unknown	0 0 3 2 0	0	1
shadow	4.6	unknown	0 0 1 0 0	0	0

Showing 1 to 9 of 9 entries (filtered from 42 total entries)

Previous 1 Next

Vigiles: PLUS – *adds collaboration, sorting and filtering*



Products

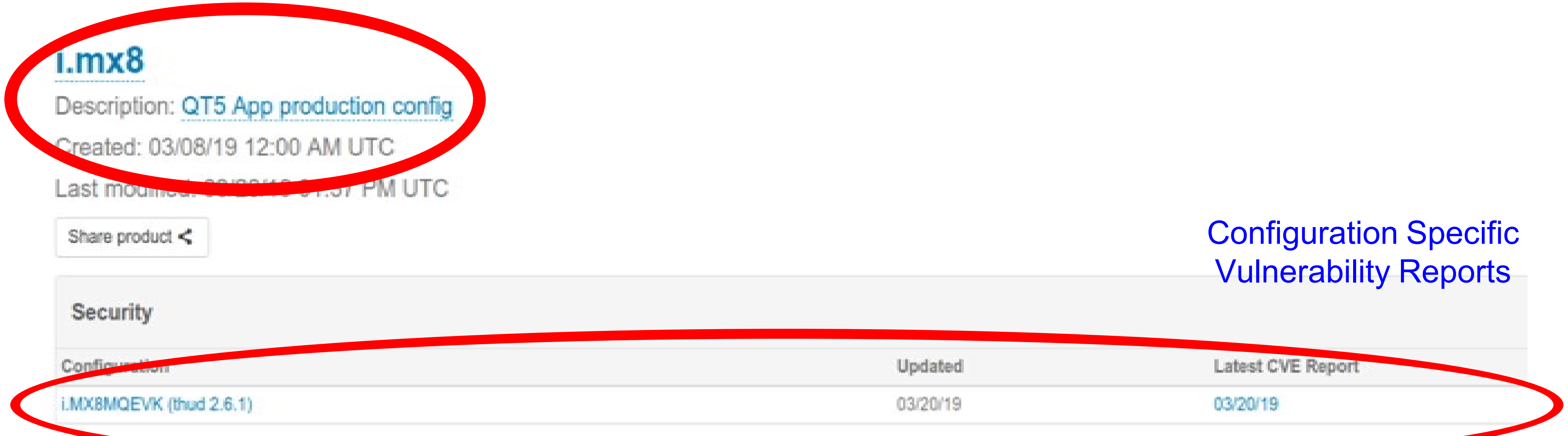
Search:

Name	Projects	Boards	Created	Last Modified
Default			03/03/19 02:39 PM UTC	03/14/19 02:39 PM UTC
i.mx6	Secure platform	i.mx6	03/07/19 12:00 AM UTC	03/20/19 12:00 AM UTC
i.mx8	QT5 APP	i.mx8	03/08/19 12:00 AM UTC	03/20/19 01:19 PM UTC
ls1021		ls1021	03/01/19 12:00 AM UTC	03/20/19 12:00 AM UTC

Add new product

Team Sharing of Product Configuration and Reports

Product Source Configuration



i.mx8

Description: QT5 App production config

Created: 03/08/19 12:00 AM UTC

Last modified: 03/20/19 01:37 PM UTC

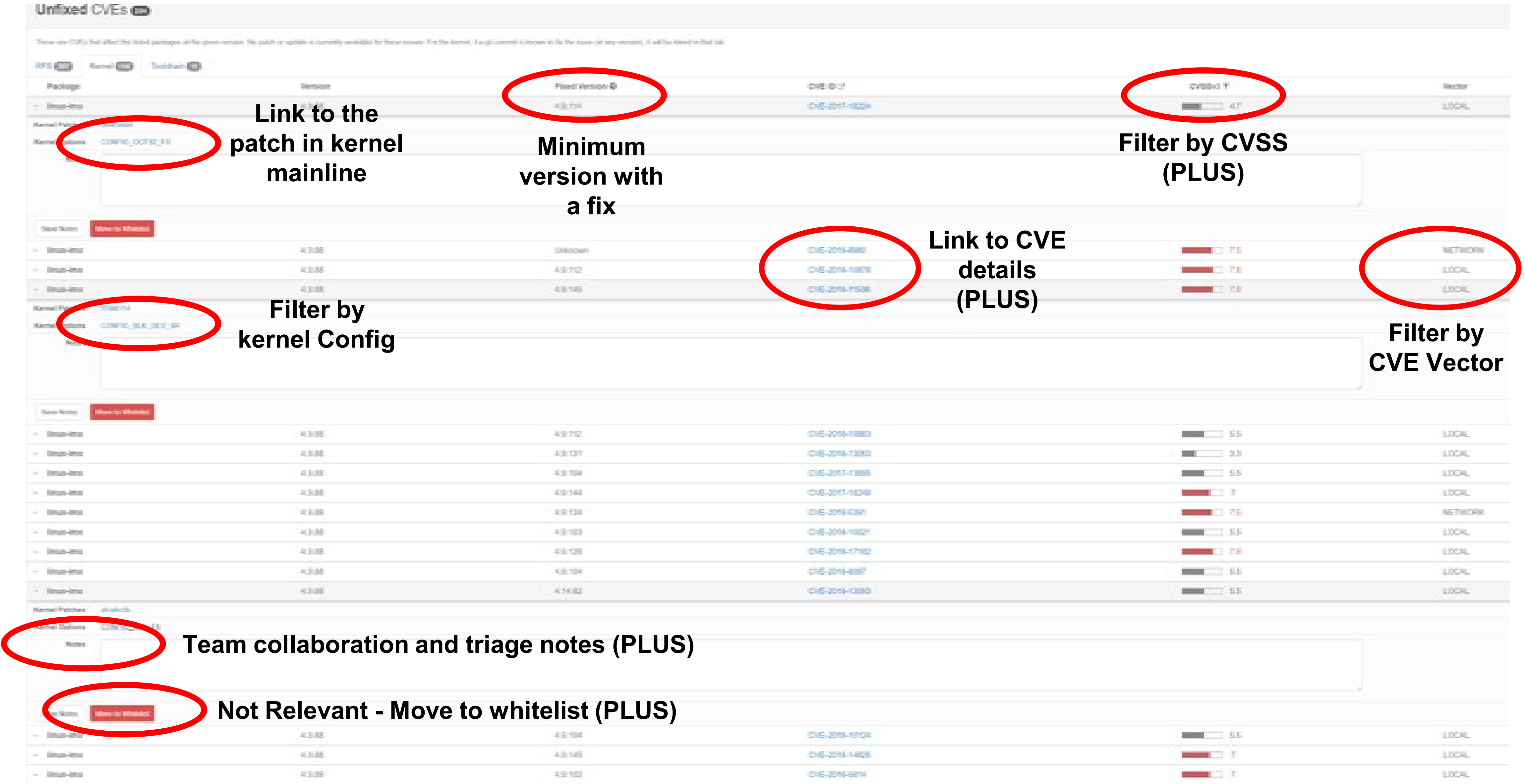
Share product <

Security

Configuration	Updated	Latest CVE Report
i.MX8MQEVK (thud 2.6.1)	03/20/19	03/20/19

Configuration Specific Vulnerability Reports

Vigiles: PRIME – Includes links to patches and more filtering



Link to the patch in kernel mainline

Minimum version with a fix

Filter by CVSS (PLUS)

Link to CVE details (PLUS)

Filter by kernel Config

Filter by CVE Vector

Team collaboration and triage notes (PLUS)

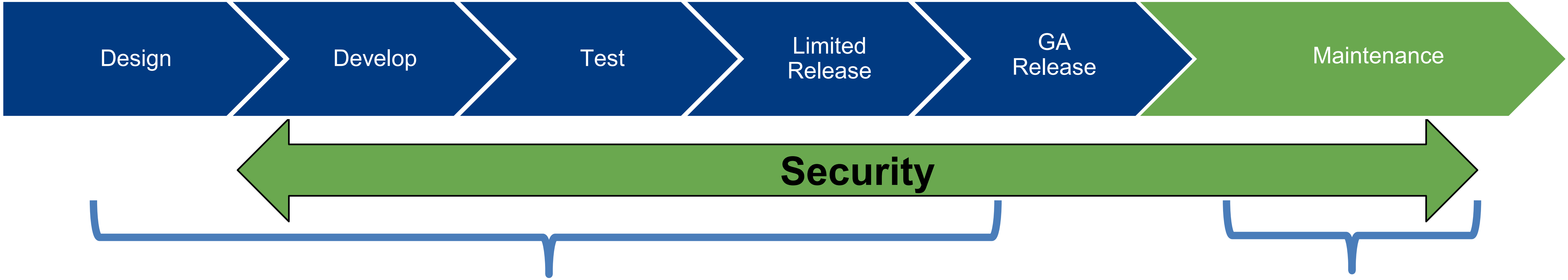
Not Relevant - Move to whitelist (PLUS)

Triaging vulnerabilities

- Important step in vulnerability assessment
- Collaborative – internal and external stakeholders
- Tracking triage changes over time with history log
- Which CVEs to address driven by requirements, policies and certifications
- Ability to manage whitelisted CVEs per product
- Triage reports for security scans can be attached to release documentation

Triage info provides justifications for why certain actions on CVE vulnerabilities were taken or not

Solution: Shift Security Left and Stretch Right
Active, Continuous Security at Every Stage of SDLC



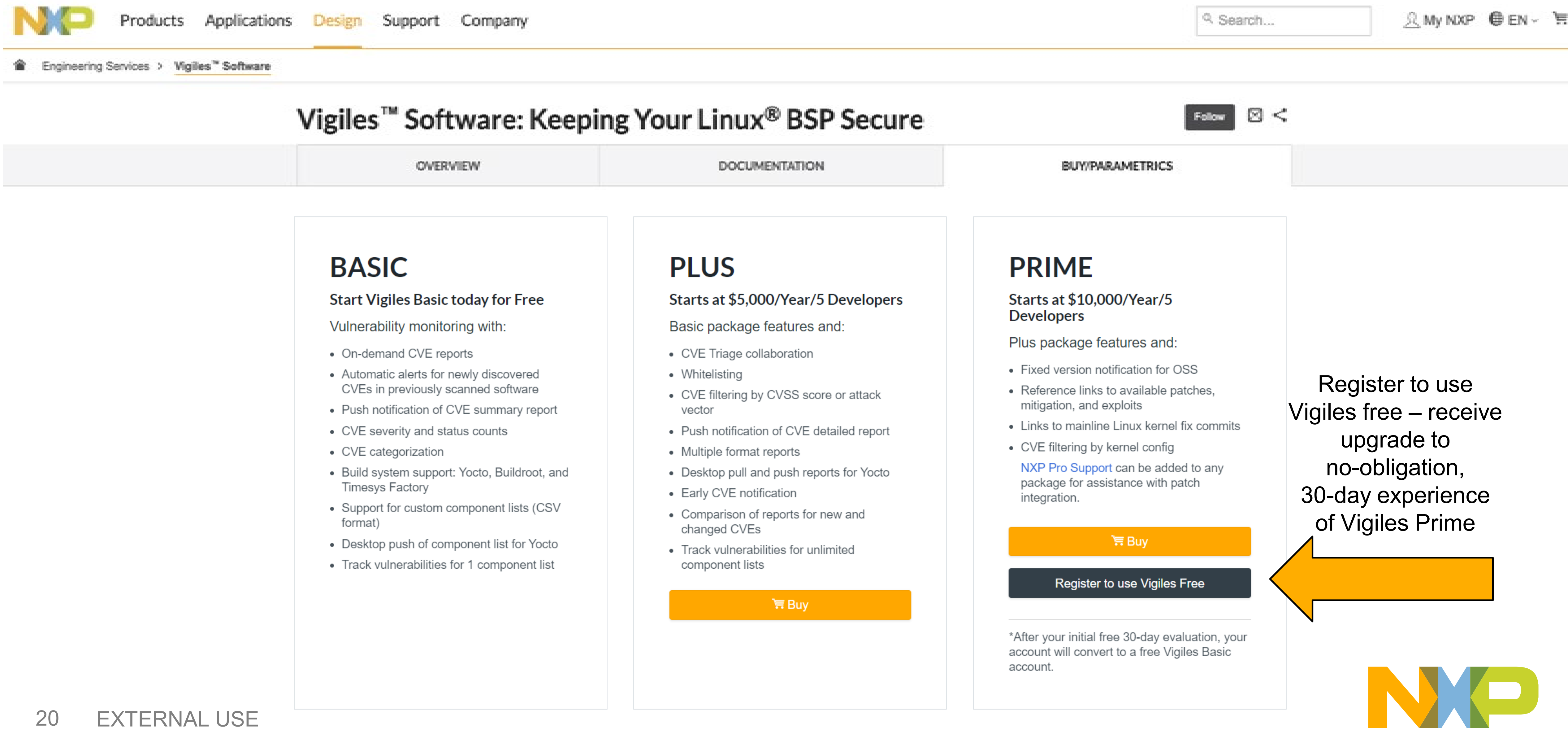
Security in design, development, testing

- Security tools that are aligned with development workflows and tools
- Highly accurate vulnerability identification for all versions, all components, all branches
- Vulnerability info is part of release

Ongoing developer-driven security maintenance

- Must conduct continuous vulnerability monitoring
- Patches & updates should be continuously monitored

How to start with Vigiles – www.nxp.com/vigiles



Vigiles™ Software: Keeping Your Linux® BSP Secure

BASIC

Start Vigiles Basic today for Free

Vulnerability monitoring with:

- On-demand CVE reports
- Automatic alerts for newly discovered CVEs in previously scanned software
- Push notification of CVE summary report
- CVE severity and status counts
- CVE categorization
- Build system support: Yocto, Buildroot, and Timesys Factory
- Support for custom component lists (CSV format)
- Desktop push of component list for Yocto
- Track vulnerabilities for 1 component list

PLUS

Starts at $5,000/Year/5 Developers

Basic package features and:

- CVE Triage collaboration
- Whitelisting
- CVE filtering by CVSS score or attack vector
- Push notification of CVE detailed report
- Multiple format reports
- Desktop pull and push reports for Yocto
- Early CVE notification
- Comparison of reports for new and changed CVEs
- Track vulnerabilities for unlimited component lists

Buy

PRIME

Starts at $10,000/Year/5 Developers

Plus package features and:

- Fixed version notification for OSS
- Reference links to available patches, mitigation, and exploits
- Links to mainline Linux kernel fix commits
- CVE filtering by kernel config

NXP Pro Support can be added to any package for assistance with patch integration.

Buy

Register to use Vigiles Free

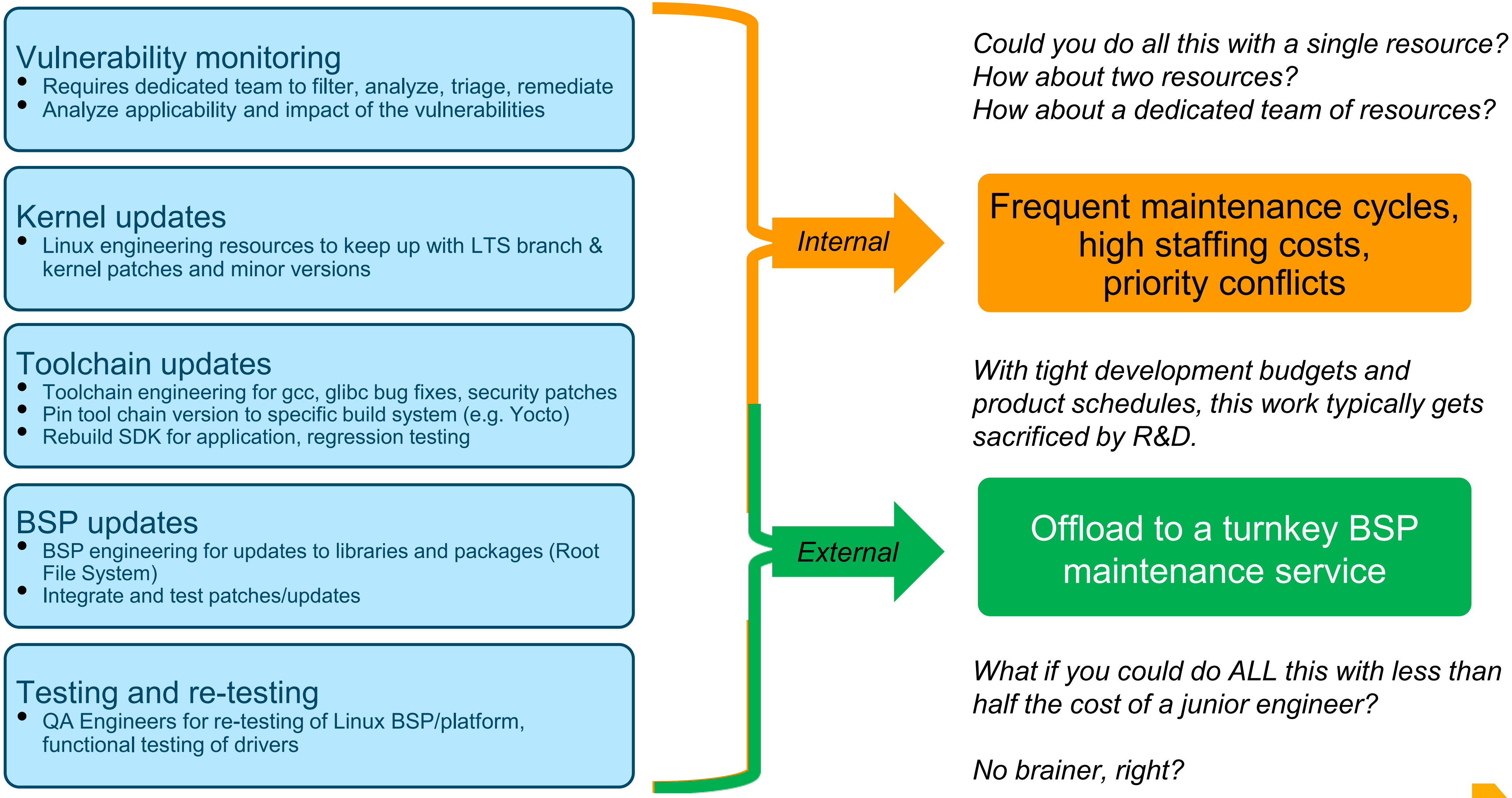
*After your initial free 30-day evaluation, your account will convert to a free Vigiles Basic account.

Register to use Vigiles free – receive upgrade to no-obligation, 30-day experience of Vigiles Prime

Benefits of using NXP Vigiles

- **Improved security**
  - *More coverage, better accuracy, early notification*
- **Time saved in monitoring**
  - *Identifies/notifies on newly discovered CVEs **and** fixes*
- **Reduced triage burden**
  - *Advanced filtering, fewer false positives, identifies already fixed CVEs*
- **Workflow management**
  - *History, collaboration tools, notes, whitelist, exported reports*
- **Integrates into engineering process**
  - *Plugs into Yocto, and a vulnerability scan can be triggered for every build*
- **Simplified, efficient vulnerability maintenance & continuous monitoring**
  - *Filters CVEs to only those that matter, tools for rapid investigation and mitigation*

BSP Maintenance Tasks and Staffing Considerations:



Vulnerability monitoring

- Requires dedicated team to filter, analyze, triage, remediate
- Analyze applicability and impact of the vulnerabilities

Kernel updates

- Linux engineering resources to keep up with LTS branch & kernel patches and minor versions

Toolchain updates

- Toolchain engineering for gcc, glibc bug fixes, security patches
- Pin tool chain version to specific build system (e.g. Yocto)
- Rebuild SDK for application, regression testing

BSP updates

- BSP engineering for updates to libraries and packages (Root File System)
- Integrate and test patches/updates

Testing and re-testing

- QA Engineers for re-testing of Linux BSP/platform, functional testing of drivers

Could you do all this with a single resource?
How about two resources?
How about a dedicated team of resources?

Internal

Frequent maintenance cycles, high staffing costs, priority conflicts

With tight development budgets and product schedules, this work typically gets sacrificed by R&D.

External

Offload to a turnkey BSP maintenance service

What if you could do ALL this with less than half the cost of a junior engineer?

No brainer, right?

More information

- Visit www.NXP.com/Vigiles
- Sign up for a free trial
- Review your BSP to see how well you are *(not)* covered!

Have questions or need help? Write us at prosupport@nxp.com

Thank You!

Q & A

SECURE CONNECTIONS
FOR A SMARTER WORLD