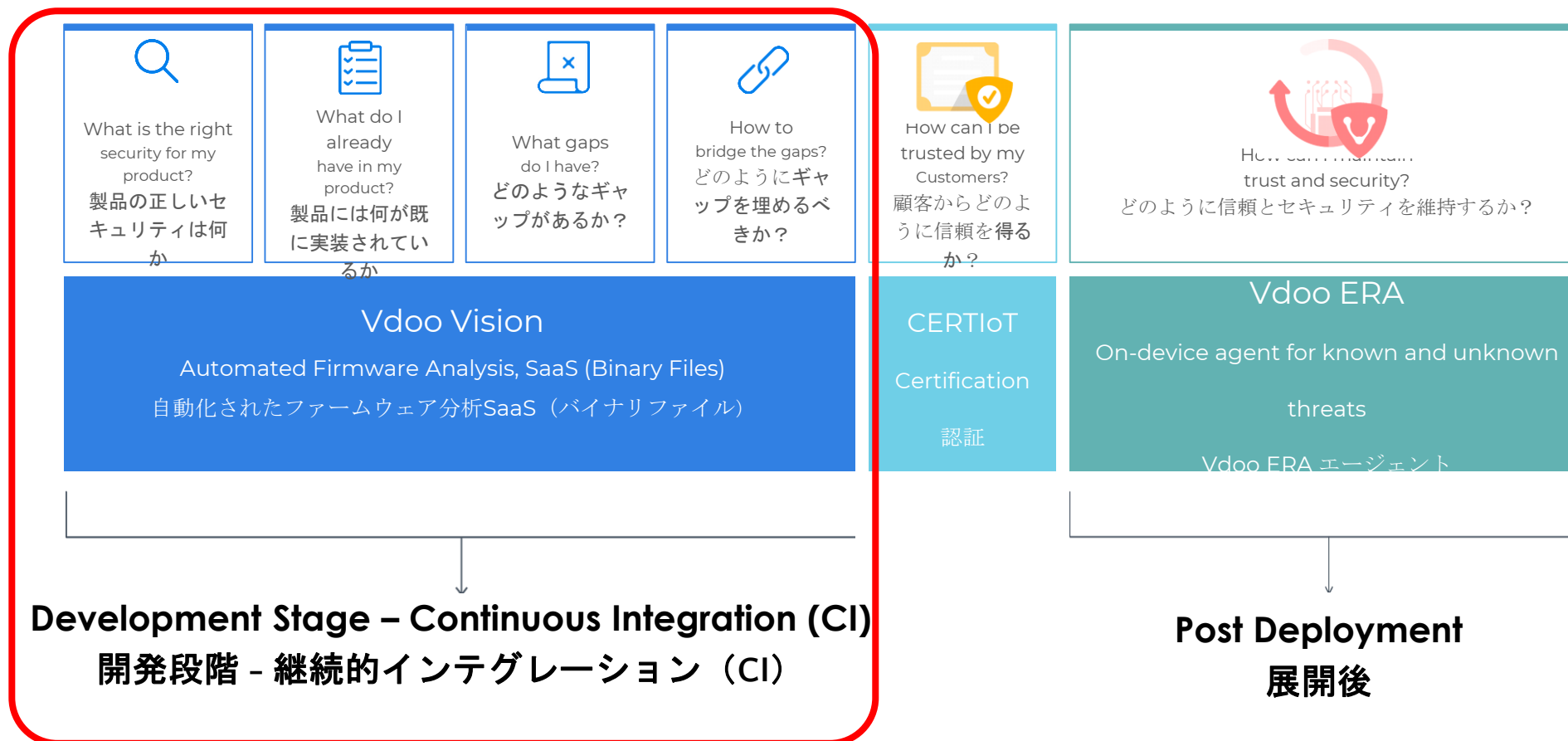


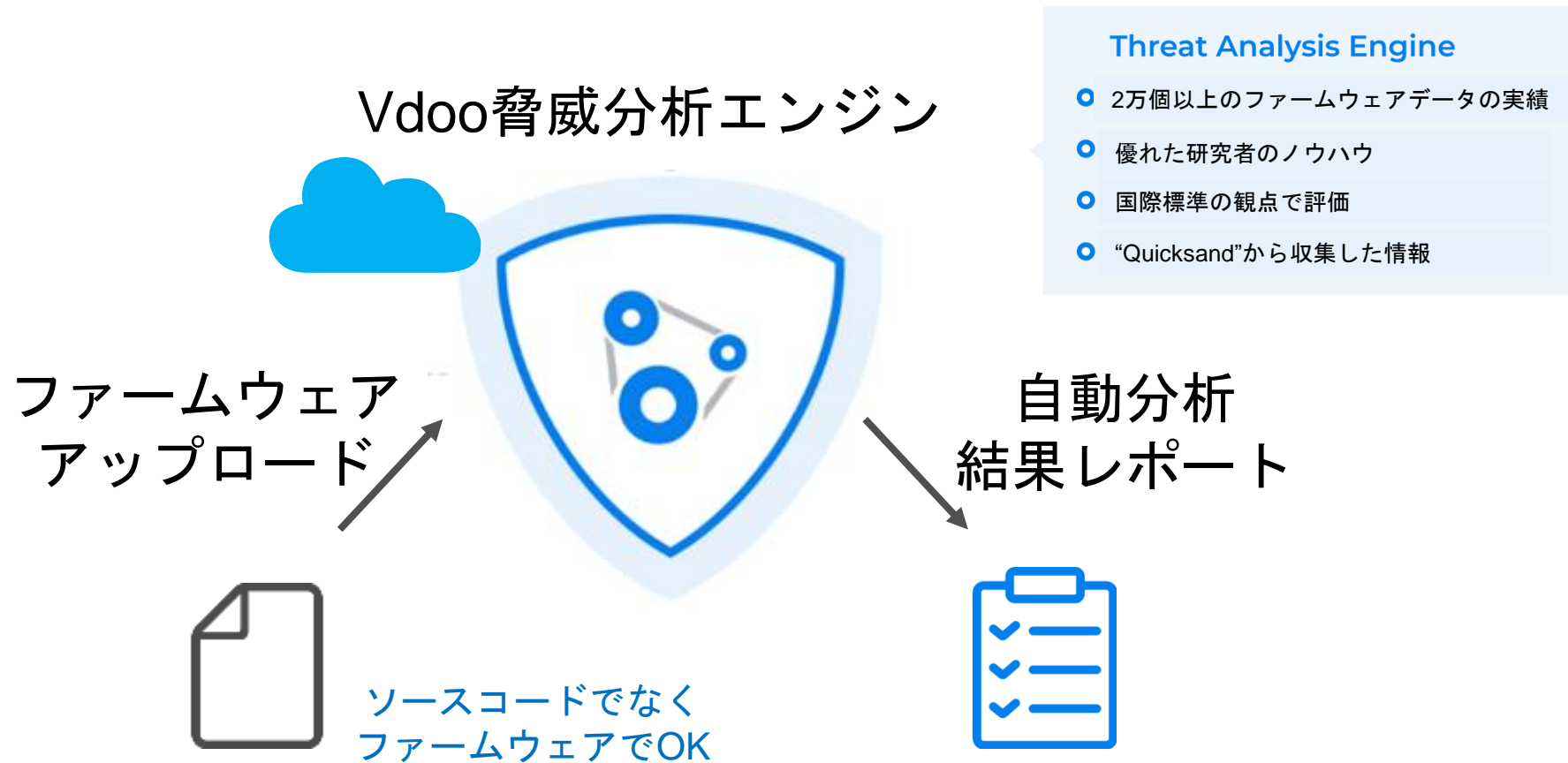
# FW脆弱性検査「Vdoo Vision」 「脆弱性対策クイックレポートサービス」のご紹介

# 開発段階 : Vdoo Vision

開発段階で脆弱性を解析し、サイバー攻撃に対するセキュリティソリューションを提供します。



IoTデバイスのファームウェアをSaaSにアップロードすると、自動的に分析し、レポートを提出します。

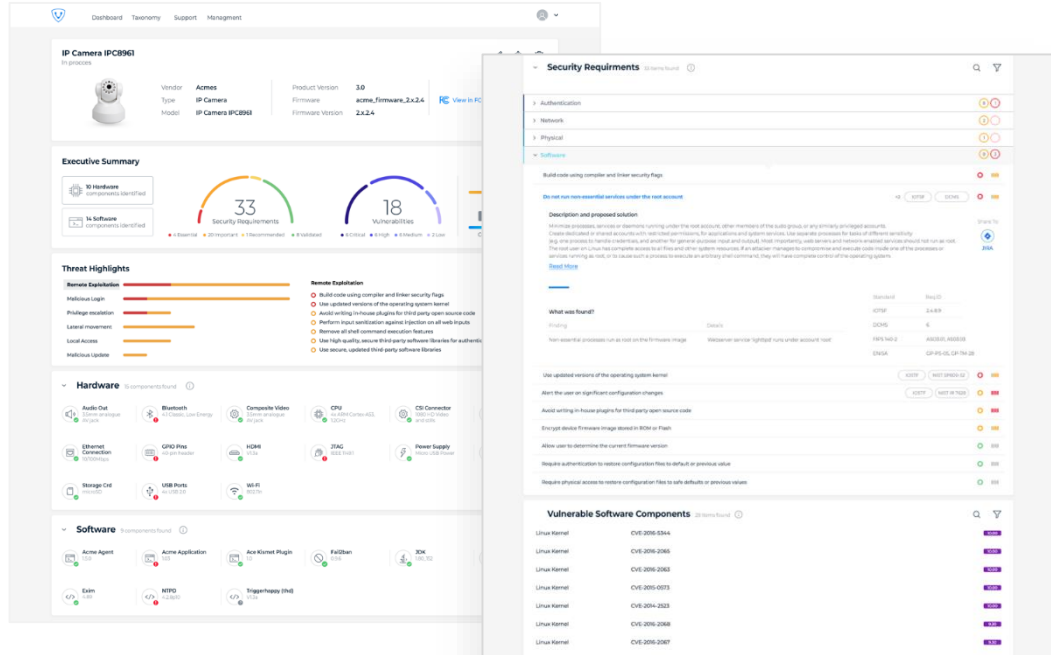


# Vdoo Vision 分析レポート(例)

レポートのガイダンスに提示された項目を改善していくことで、漏れなくセキュリティ対策を実現できます。

## CCDS・NIST等の基準に準拠

- ベンダーダッシュボード
- エグゼクティブサマリ
- リスクアセスメント
- ハードウェア  
構成リスト
- ソフトウェア  
構成リスト
- 詳細なガイダンス
- CI/CDとの統合



- Security Essentials の欠如
- 欠陥のあるセキュリティ・アーキ  
テクチャ
- 望ましくないプロセスとサービス
- 間違った構成
- バックドアと組み込みの認証鍵が  
残っている状態を指摘
- サードパーティモジュールの  
既知の脆弱性
- 追加の疑わしい脆弱性

ファームウェア分析結果レポートには、  
 - どのような攻撃要因があるのか  
 - 何に取り組むべきなのか  
 - 各国・地域の規格・基準に準拠しているか  
 等の改善リストに優先順位を付けて、その解決に向けたガイダンスを提示します。

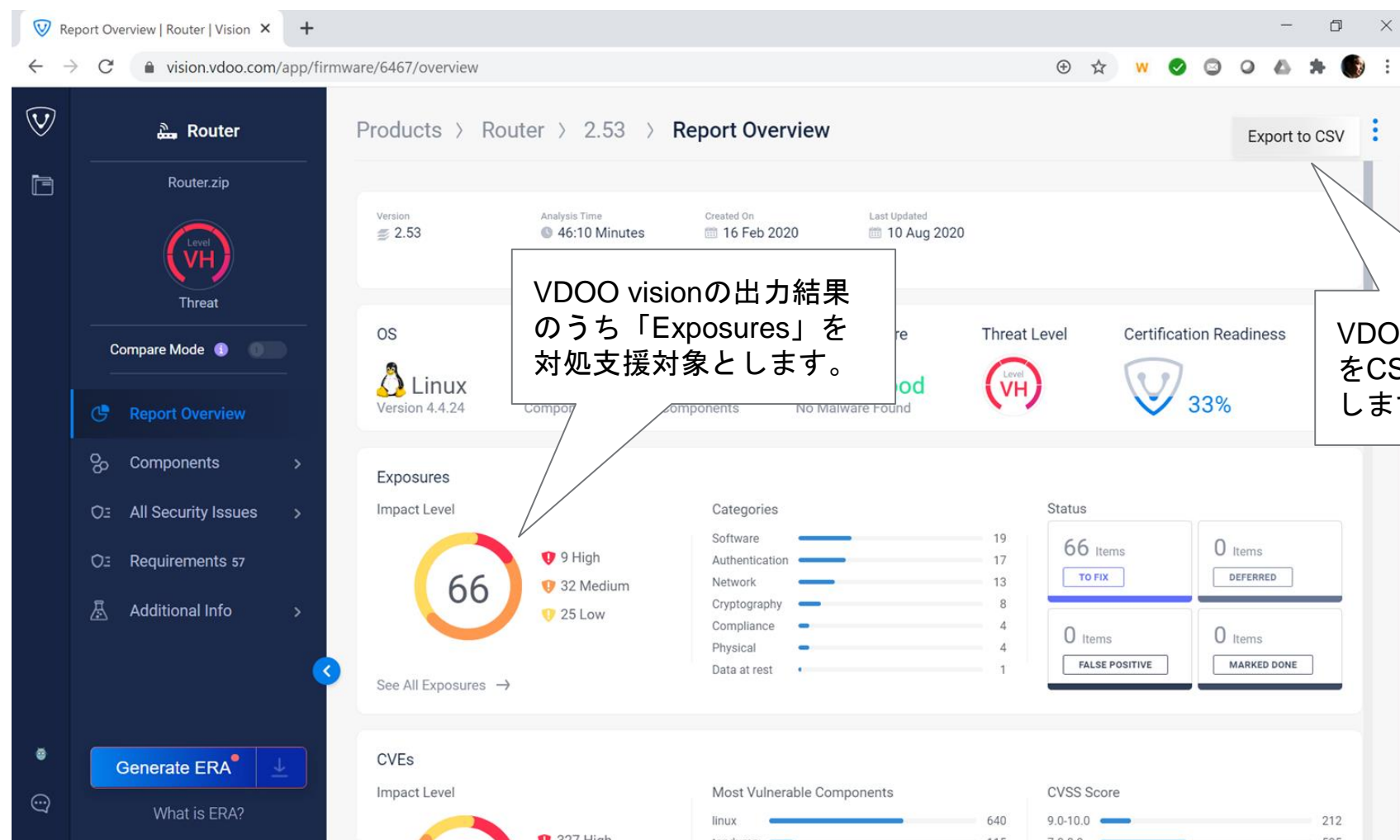
日々進化し複雑化していくサイバーセキュリティ対策要件  
HWに対する要件も増えてきております。企画・設計する前に現状把握することが第一歩。  
対象となる規格要件に対するGAP分析及び対処方法についてレポート提供します。

## <主な報告内容>

- リスクエリアの特定と、デバイス特有の詳細ガイドラインによる修正方法を優先付け
- 詳細なデバイスバイナリ分析で既知の脆弱性やゼロデイ脆弱性の可能性を検知
- サプライヤに依存せずにサードパーティ製品やコンポーネントの脆弱性をアセスメント

- サービス内容
  - Vdooでバイナリ診断を適用した際に出力されるレポートに対して、対処策の分類をします。
  - 対策を進めるうえで一般的な機器に求められる必要最小限な対策に絞り込んだアドバイスを診断実施から約二週間で提示します。
  - 対処策の分類のうち、Yoctoでの対応が可能と判断した場合にYoctoレシピもしくはコンフィグレーションでの対応策を提示します。
- サービスを受けるために必要な情報
  - Vdooでのバイナリ診断結果
  - Vdooが表示する「What should I do?」レポート
- 本サービスによる効果
  - Vdooの「What should I do?」レポートでは個別の対処策を提示していますが、これをYoctoレシピもしくはコンフィグレーションに適用することで、**プロダクトのセキュリティ対策を継続的に適用することができ、さらに他プロジェクトへの転用も可能となります。**
- Visionライセンス料+時間単位でのご契約方式となります。

# 脆弱性対策クイックレポートサービスイメージ 1/4



Report Overview | Router | Vision

vision.vdoo.com/app/firmware/6467/overview

Products > Router > 2.53 > Report Overview

Export to CSV

Version 2.53 Analysis Time 46:10 Minutes Created On 16 Feb 2020 Last Updated 10 Aug 2020

OS Linux Version 4.4.24

Threat Level Level VH

Certification Readiness 33%

Exposures Impact Level

66

9 High 32 Medium 25 Low

Categories

Software	19
Authentication	17
Network	13
Cryptography	8
Compliance	4
Physical	4
Data at rest	1

Status

66 Items TO FIX	0 Items DEFERRED
0 Items FALSE POSITIVE	0 Items MARKED DONE

CVEs Impact Level

Most Vulnerable Components

linux	640
redpanda	115

CVSS Score

9.0-10.0	212
7.0-8.9	505

Generate ERA

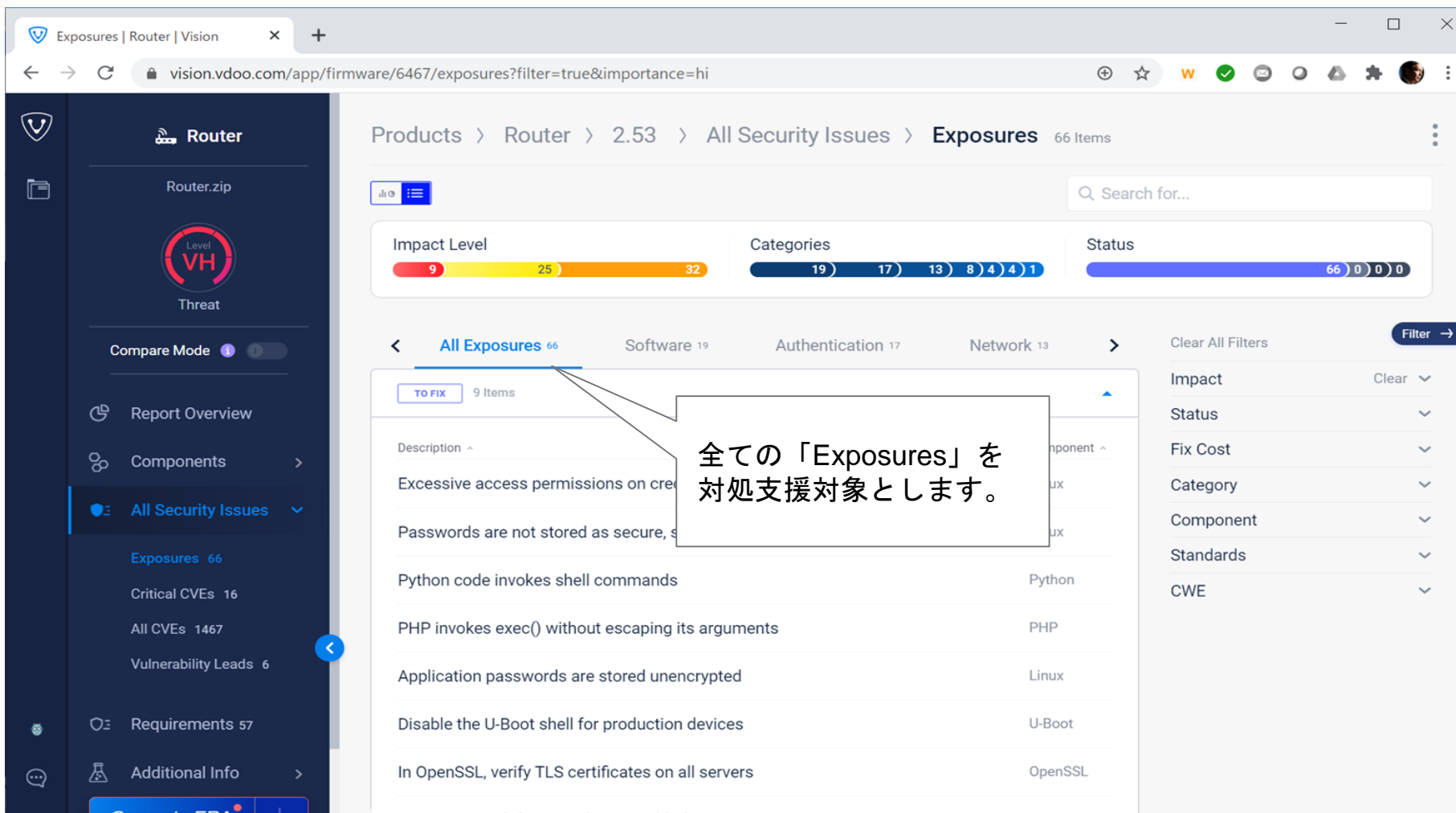
What is ERA?

VDOO visionの出力結果のうち「Exposures」を対処支援対象とします。

VDOO visionの解析結果をCSVファイルに吐き出します。

## Vdoo vision のOverviewレポート

# 脆弱性対策クイックレポートサービスイメージ 2/4



Exposures | Router | Vision

vision.vdoo.com/app/firmware/6467/exposures?filter=true&importance=hi

Products > Router > 2.53 > All Security Issues > Exposures 66 Items

Search for...

Impact Level: 9 (Critical), 25 (High), 32 (Medium)

Categories: 19 (Software), 17 (Authentication), 13 (Network)

Status: 66 (Open), 0 (In Progress), 0 (Closed), 0 (Resolved)

Filter: All Exposures 66, Software 19, Authentication 17, Network 13

TO FIX 9 Items

Description ^

Description	Component
Excessive access permissions on create...	Linux
Passwords are not stored as secure, s...	Linux
Python code invokes shell commands	Python
PHP invokes exec() without escaping its arguments	PHP
Application passwords are stored unencrypted	Linux
Disable the U-Boot shell for production devices	U-Boot
In OpenSSL, verify TLS certificates on all servers	OpenSSL

Impact: Clear

Status: Clear

Fix Cost: Clear

Category: Clear

Component: Clear

Standards: Clear

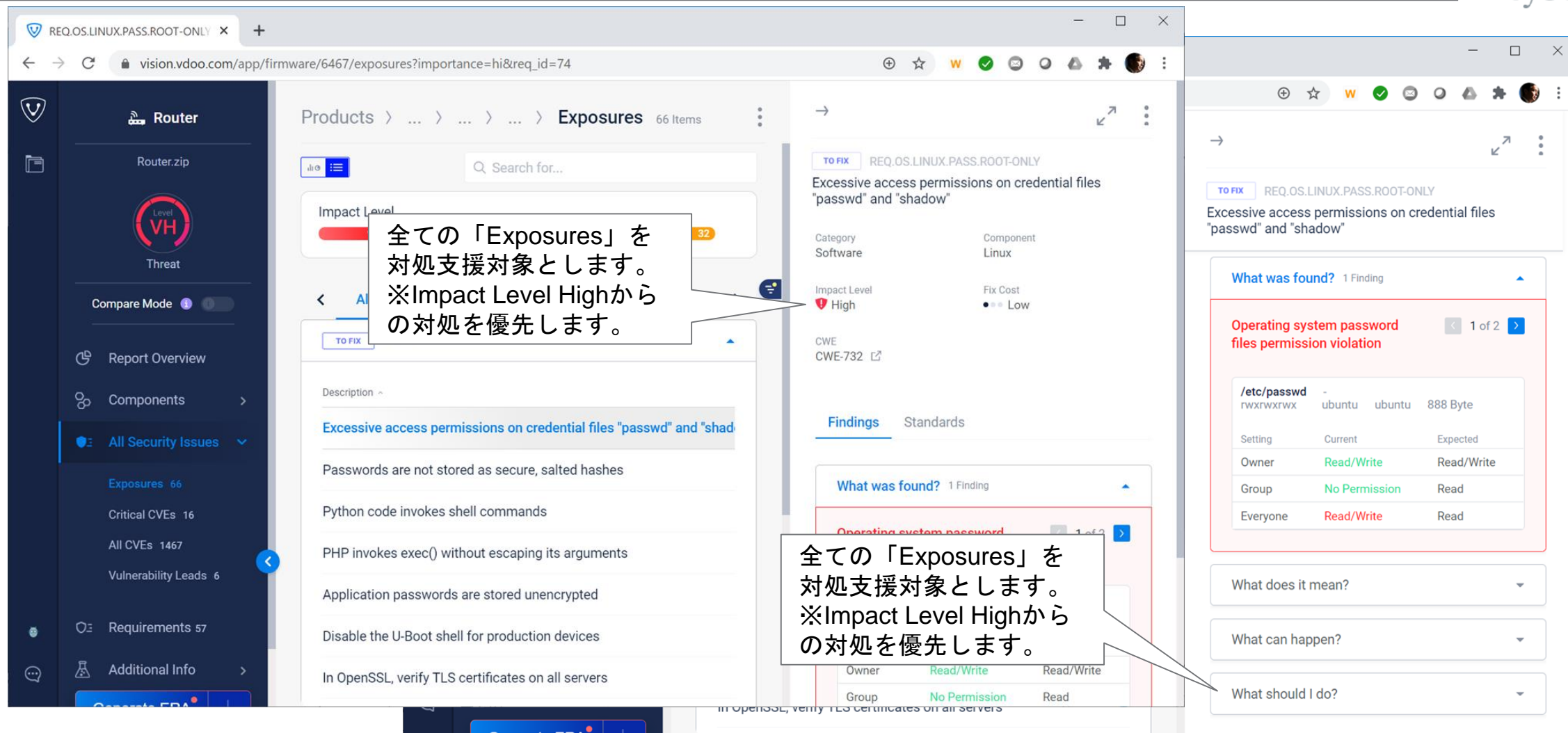
CWE: Clear

全ての「Exposures」を対処支援対象とします。

Vdoo vision のExposuresリポート



# 脆弱性対策クイックレポートサービスイメージ 3/4



The screenshot displays the Vdoo vision web interface for a Router. The left sidebar shows navigation options like 'Router', 'Report Overview', and 'All Security Issues'. The main content area shows a list of exposures, with one selected: 'Excessive access permissions on credential files "passwd" and "shadow"'. This exposure is categorized as 'Software' on 'Linux' with a 'High' impact level. A detailed view of this finding is shown on the right, including a table of file permissions for '/etc/passwd'.

Setting	Current	Expected
Owner	Read/Write	Read/Write
Group	No Permission	Read
Everyone	Read/Write	Read

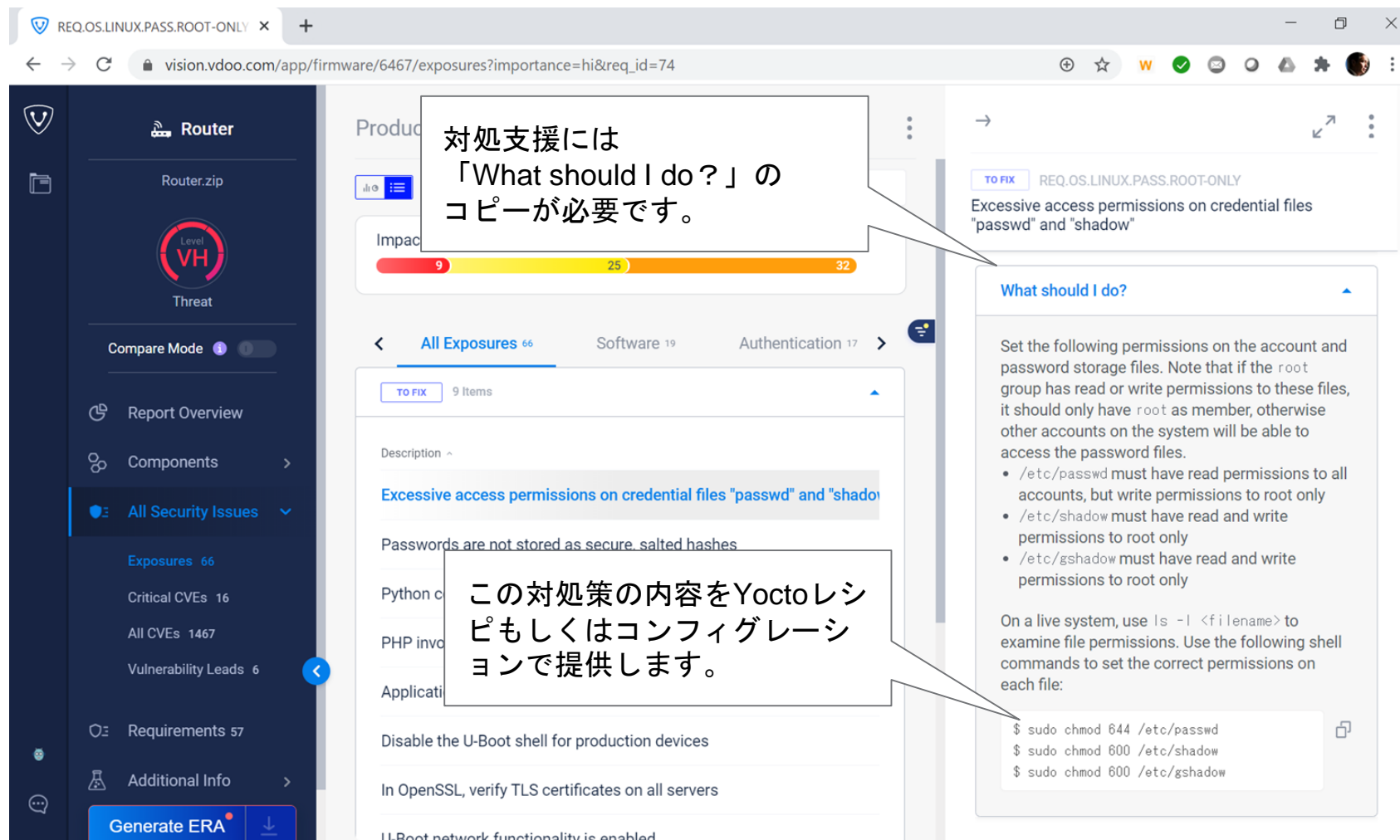
Two callout boxes with Japanese text are overlaid on the image:

全ての「Exposures」を  
対処支援対象とします。  
※Impact Level Highから  
の対処を優先します。

全ての「Exposures」を  
対処支援対象とします。  
※Impact Level Highから  
の対処を優先します。

Vdoo vision のExposuresレポート

# 脆弱性対策クイックレポートサービスイメージ 4/4



The screenshot shows the Vdoo vision web interface for a security report. The left sidebar contains navigation options like 'Router', 'Report Overview', 'Components', 'All Security Issues', and 'Requirements'. The main content area displays a list of exposures, with one selected: 'Excessive access permissions on credential files "/>

対処支援には「What should I do?」のコピーが必要です。

この対処策の内容をYoctoレシピもしくはコンフィグレーションで提供します。

**What should I do?**

Set the following permissions on the account and password storage files. Note that if the `root` group has read or write permissions to these files, it should only have `root` as member, otherwise other accounts on the system will be able to access the password files.

- `/etc/passwd` must have read permissions to all accounts, but write permissions to root only
- `/etc/shadow` must have read and write permissions to root only
- `/etc/gshadow` must have read and write permissions to root only

On a live system, use `ls -l <filename>` to examine file permissions. Use the following shell commands to set the correct permissions on each file:

```
$ sudo chmod 644 /etc/passwd
$ sudo chmod 600 /etc/shadow
$ sudo chmod 600 /etc/gshadow
```

Vdoo vision のExposures リポート

## [課題]

Operating system password files permission violation

## [対策]

ユーザレシピ内でイメージ作成後の処理コマンドとして、以下を設定します。

```
$ cat repos/meta-user/recipes-images/images/core-image-minimal.bbappend
ROOTFS_POSTPROCESS_COMMAND += "set_shadow_files_permission; "
set_shadow_files_permission () {
    chmod 644 ${IMAGE_ROOTFS}/etc/shadow
    chmod 600 ${IMAGE_ROOTFS}/etc/gshadow
    chmod 600 ${IMAGE_ROOTFS}/etc/passwd
}
```

## [備考]

この設定により、起動イメージ作成時に適切なパーミッションが設定されます。この設定はライブラリのバージョンによる影響を受けません。ただし、OSのメジャーバージョンが変更になった場合には、ファイル構成の変更などへの対応が必要となります。

お問い合わせはこちら

---



サイバートラスト株式会社  
IoT 総合お問い合わせ窓口  
[iot-contact@cybertrust.co.jp](mailto:iot-contact@cybertrust.co.jp)



# 信頼とともに

## 留意事項

本資料に記載されている会社名、製品名、サービス名は、当社または各社、各団体の商標もしくは登録商標です。  
その他本資料に記載されているイラスト・ロゴ・写真・動画・ソフトウェア等は、当社または第三者が有する知的財産権やその他の権利により守られております。  
お客様は、当社が著作権を有するコンテンツについて、特に定めた場合を除き、複製、改変、頒布などを行うことはできません。  
本資料に記載されている情報は予告なしに変更されることがあります。また、時間の経過などにより記載内容が不正確となる場合がありますが、当社は、当該情報を更新する義務を負うものではありません。