

WINDRV R

# Wind River Studio Linux Services CVEスキャン

サンプルのSBOMファイルを使って  
CVEスキャンを試してみましょう！

## Wind River Studio Security Scanner

A professional-grade security vulnerability scanner, specifically curated to meet the unique needs of embedded systems.

- Secure, web-based service
- GUI with easy-to-understand dashboard
- Analysis of vulnerabilities, licensing, versioning, and community resources
- Collaboration and reporting

FREE CVE SCANNER

LOG IN

← TRY

アカウント作成完了の連絡がありましたら、リンク先ページからログインください。

## Dashboard /

0

VULNERABLE PROJECTS



0

VULNERABLE PACKAGES



0

VULNERABILITIES



### SUMMARY /

0

Policy Violation  
Projects

0

Policy Violation  
Packages

0

Policy Violation  
CVEs

0

CISA  
CVEs



LIVE CHAT

ログイン後、Dashboard（ダッシュボード）ページへ遷移します。

## Dashboard /

0  
VULNERABLE PROJECTS



0  
VULNERABLE PACKAGES



0  
VULNERABILITIES



### SUMMARY /

0

Policy Violation  
Projects

0

Policy Violation  
Packages

0

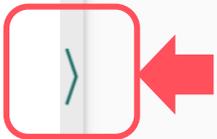
Policy Violation  
CVEs

0

CISA  
CVEs



LIVE CHAT



左サイドの > をクリックして、サイドバーを開きます。

Dashboard

Groups

Projects

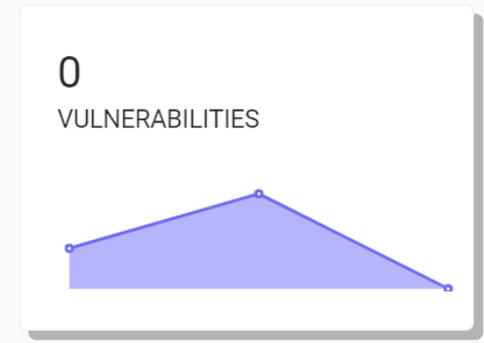
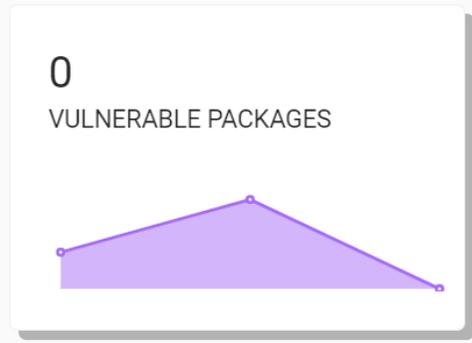
Packages

Vulnerabilities

Policy Management

Settings

# Dashboard /



SUMMARY /

0	0	0	0
Policy Violation Projects	Policy Violation Packages	Policy Violation CVEs	CISA CVEs

LIVE CHAT

Projects (プロジェクト) をクリックします。

Dashboard

Groups

Projects

Packages

Vulnerabilities

Policy Management

Settings

## Projects /

[+ NEW PROJECT](#)0  
VULNERABLE PROJECTS0  
VULNERABLE PACKAGES0  
VULNERABILITIES

Q Project

PROJECT NAME	GROUP NAME	LAST SCANNED	LAST SBOM UPDATED	POLICY VIOLA
--------------	------------	--------------	-------------------	--------------

Create your first project!



LIVE CHAT

右上の [+ NEW PROJECT](#) をクリックし、プロジェクトを開きます。

[Dashboard](#)[Groups](#)[Projects](#)[Packages](#)[Vulnerabilities](#)[Policy Management](#)[Settings](#)

## Untitled Project /

Project Name \*

Project Description

0/500

Project File \*

SBOM, package details, or manifest.

[Show me how to create a sbom](#)

[VIEW A SAMPLE PROJECT](#)

  
Drag files here to add  
or  
[CHOOSE FILES](#)

[VIEW A SAMPLE PROJECT](#)

をクリックし、サンプルファイルをダウンロードします。

Dashboard

Groups

Projects

Packages

Vulnerabilities

Policy Management

Settings

## Untitled Project /

Project Name \*

Project Description

0/500

Project File \*

 Yocto-Zeus-3.0.4.spdx.json

Success! File Uploaded.

SAVE &amp; SCAN



ダウンロードが成功したら、 **SAVE & SCAN** をクリックします。

Dashboard

Groups

Projects

Yocto-Zeus-3.0.4

Packages

Vulnerabilities

Policy Management

Settings

## Yocto-Zeus-3.0.4 /

Info

Operating System:

Version:

Last Scanned: Running [CANCEL SCAN](#)

Last SBOM Updated: Feb 6, 2024

[UPDATE PROJECT FILE](#)

Dashboard

Packages

CVEs

Policies

Scan in  
progress... CVE scan in progress...

クリック後、CVEスキャンが開始されます。スキャンは数分で完了します。

Dashboard

Groups

Projects

Yocto-Zeus-3.0.4

Packages

Vulnerabilities

Policy Management

Settings

# Yocto-Zeus-3.0.4 /

Info

Operating System: Yocto

Version: 3.0.4

Last Scanned: Feb 6, 2024 15:20

Last SBOM Updated: Feb 6, 2024

UPDATE PROJECT FILE

Dashboard

Packages

CVEs

Policies

SUMMARY /

99

All Packages

0

Allowlisted Packages

1415

All CVEs

1390

Vulnerable CVEs

0

Allowlisted CVEs



LIVE CHAT

スキャンが完了したら、結果をご覧ください。

# CVEスキャン結果の見方

Dashboard

Groups

Projects

Yocto-Zeus-3.0.4

Packages

Vulnerabilities

Policy Management

Settings

## Yocto-Zeus-3.0.4 /

Info

Operating System: Yocto

Version: 3.0.4

Last Scanned: Feb 6, 2024 15:20

Last SBOM Updated: Feb 6, 2024

UPDATE PROJECT FILE

Dashboard

Packages

CVEs

Policies

SUMMARY /

99

All  
Packages

0

Allowlisted  
Packages

1415

All  
CVEs

1390

Vulnerable  
CVEs

0

Allowlisted  
CVEs

LIVE CHAT

Dashboard (ダッシュボード) タブでは、スキャンしたSBOMファイルに含まれる Packagesや特定されたCVEを確認することができます。

Operating System: Yocto

Version: 3.0.4

Last Scanned: Feb 6, 2024 15:20

Last SBOM Updated: Feb 6, 2024

[UPDATE PROJECT FILE](#)

Dashboard

Packages

CVEs

Policies

SUMMARY /

99

All  
Packages

0

Allowlisted  
Packages

1415

All  
CVEs

1390

Vulnerable  
CVEs

0

Allowlisted  
CVEs

VULNERABILITY SEVERITY /

43

Critical

423

High

532

Medium

36

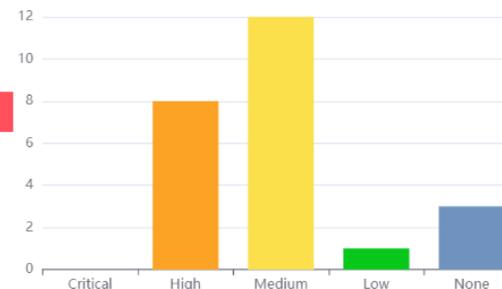
Low

356

None

CVEs MITIGATED WITHIN LAST

Day Week Month Year



Last Updated: 31 minutes 18 seconds ago.

「VULNERABILITY SEVERITY（脆弱性の影響度）」では、「Critical」「High」「Medium」「Low」「None」に該当する CVEを確認することができます。

Operating System: Yocto

Version: 3.0.4

Last Scanned: Feb 6, 2024 15:20

Last SBOM Updated: Feb 6, 2024

[UPDATE PROJECT FILE](#)

Dashboard

Packages

CVEs

Policies

SUMMARY /

99

All Packages

0

Allowlisted Packages

1415

All CVEs

1390

Vulnerable CVEs

0

Allowlisted CVEs

VULNERABILITY SEVERITY /

43

Critical

36

Low

423

High

532

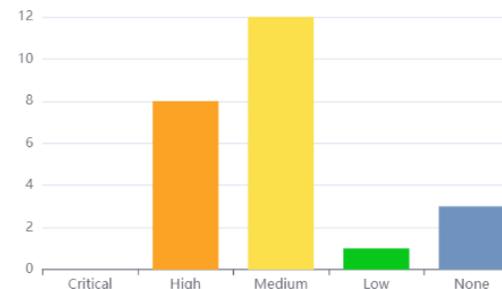
Medium

356

None

CVEs MITIGATED WITHIN LAST

Day Week Month Year



Last Updated: 31 minutes 18 seconds ago.

今回のスキャンでは、Criticalに該当するCVEが43件あったことが分かります。  
43をクリックすると、該当するCVEの詳細を確認できます。

ONLY SHOW STARRED ☆

COLUMNS

EXPORT

<input type="checkbox"/>	SEVERITY	CVE ID	PACKAGE	CVSS 3 SCORE	WR SOLUTION	PUBLISHED	MODIFIED	STATUS	
<input type="checkbox"/>	★ Critical	<a href="#">CVE-2023-6816</a>	<a href="#">libx11 1.6.8</a>	9.8	No	Jan 18, 2024	Feb 5, 2024	Vulnerable	⋮
<input checked="" type="checkbox"/>	★ Critical	<a href="#">CVE-2023-45871</a>	<a href="#">linux-libc-headers...</a> +	9.8	Yes	Oct 15, 2023	Nov 11, 2023	Vulnerable	
<input type="checkbox"/>	★ Critical	<a href="#">CVE-2023-45853</a>	<a href="#">zlib 1.2.11</a>	9.8	Yes	Oct 14, 2023	Jan 25, 2024	Vulnerable	⋮
<input type="checkbox"/>	★ Critical	<a href="#">CVE-2022-48174</a>	<a href="#">busybox 1.31.0</a>	9.8	Yes	Aug 23, 2023	Aug 29, 2023	Vulnerable	⋮
<input type="checkbox"/>	★ Critical	<a href="#">CVE-2022-48565</a>	<a href="#">python3 3.7.8</a>	9.8	Yes	Aug 23, 2023	Nov 4, 2023	Vulnerable	⋮
<input type="checkbox"/>	★ Critical	<a href="#">CVE-2022-37454</a>	<a href="#">python3 3.7.8</a>	9.8	Yes	Oct 21, 2022	May 3, 2023	Vulnerable	⋮
<input type="checkbox"/>	★ Critical	<a href="#">CVE-2022-37434</a>	<a href="#">zlib 1.2.11</a>	9.8	Yes	Aug 5, 2022	Jul 19, 2023	Vulnerable	⋮
<input type="checkbox"/>	★ Critical	<a href="#">CVE-2022-2068</a>	<a href="#">openssl 1.1.1g</a>	9.8	Yes	Jun 22, 2022	Mar 2, 2023	Vulnerable	⋮
<input type="checkbox"/>	★ Critical	<a href="#">CVE-2022-1292</a>	<a href="#">openssl 1.1.1g</a>	9.8	Yes	May 4, 2022	Feb 14, 2023	Vulnerable	⋮
<input type="checkbox"/>	★ Critical	<a href="#">CVE-2021-38578</a>	<a href="#">linux-libc-headers...</a>	9.8	No	Mar 4, 2022	Aug 3, 2023	Vulnerable	⋮
<input type="checkbox"/>	★ Critical	<a href="#">CVE-2022-25315</a>	<a href="#">expat 2.2.8</a>	9.8	Yes	Feb 18, 2022	Oct 6, 2022	Vulnerable	⋮
<input checked="" type="checkbox"/>	★ Critical	<a href="#">CVE-2021-3773</a>	<a href="#">linux-libc-headers...</a> +	9.8	Yes	Feb 17, 2022	Feb 24, 2023	Vulnerable	
<input type="checkbox"/>	★ Critical	<a href="#">CVE-2022-25235</a>	<a href="#">expat 2.2.8</a>	9.8	Yes	Feb 16, 2022	Oct 8, 2022	Vulnerable	⋮
<input type="checkbox"/>	★ Critical	<a href="#">CVE-2022-25236</a>	<a href="#">expat 2.2.8</a>	9.8	Yes	Feb 16, 2022	Oct 7, 2022	Vulnerable	⋮

クリックすると、Criticalに該当するCVEのみの情報が表示されました。  
該当のCVE IDやPACKAGEをクリックして、さらに詳細情報を確認することができます。  
右上の「Export」ボタンをクリックすると、ファイルにExportすることも可能です。

Operating System: Yocto

Version: 3.0.4

Last Scanned: Feb 6, 2024 15:20

Last SBOM Updated: Feb 6, 2024

UPDATE PROJECT FILE

Dashboard

Packages

CVEs

Policies

SUMMARY /

99

All  
Packages

0

Allowlisted  
Packages

1415

All  
CVEs

1390

Vulnerable  
CVEs

0

Allowlisted  
CVEs

VULNERABILITY SEVERITY /

43

Critical

423

High

532

Medium

36

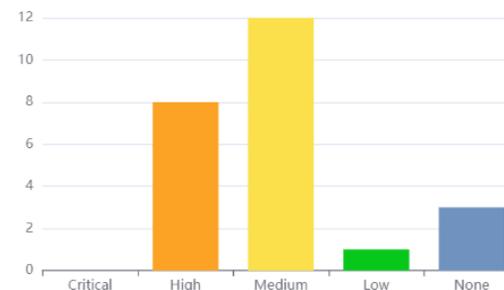
Low

356

None

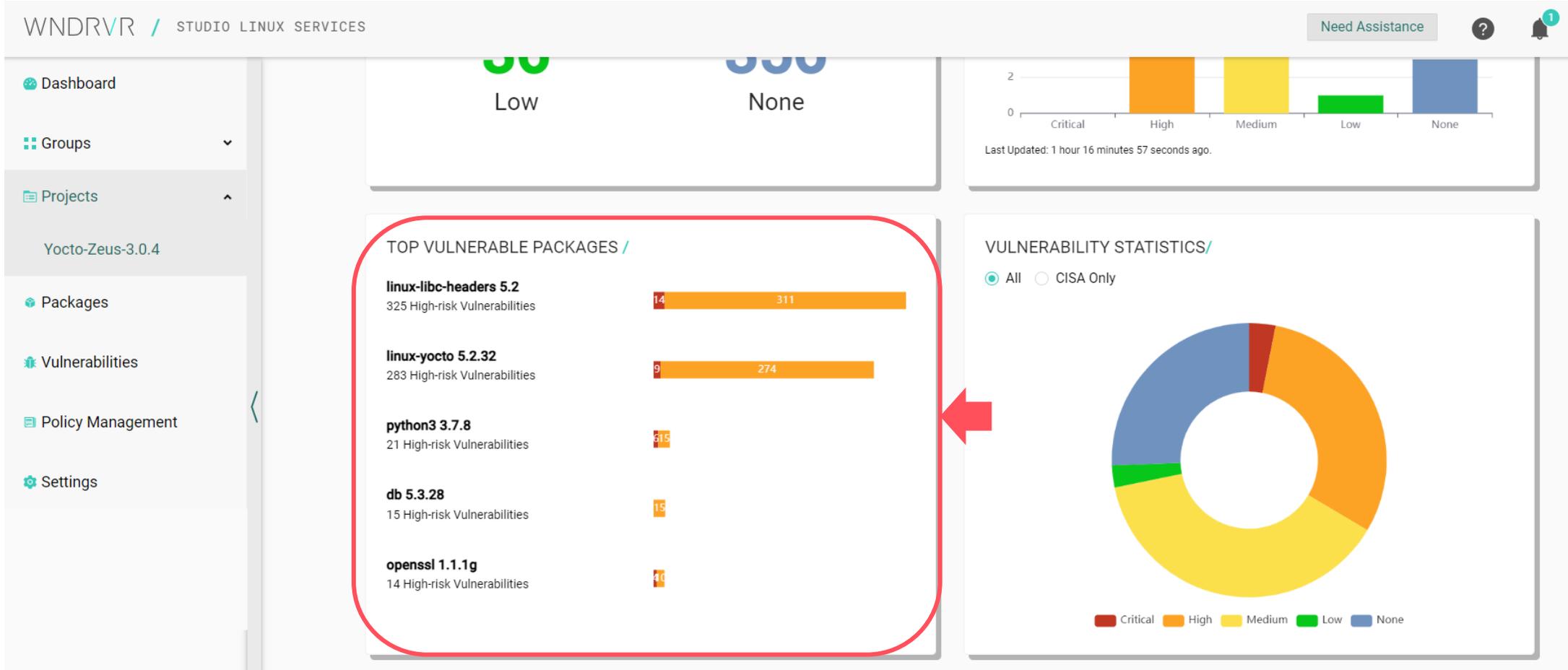
CVEs MITIGATED WITHIN LAST

Day Week Month Year



Last Updated: 31 minutes 18 seconds ago.

Dashboardに戻りましょう。「CVEs MITIGATED WITHIN LAST (緩和済みのCVE)」では、「Day」「Week」「Month」「Year」を選択すると、選択した期間に解決されたCVEを確認することができます。



「TOP VULNERABLE PACKAGES（脆弱性のあるパッケージの上位）」では、影響度の高いパッケージを確認することができます。

WINDRIVER / STUDIO LINUX SERVICES Need Assistance ? 1

- Dashboard
- Groups
- Projects
  - Yocto-Zeus-3.0.4
- Packages
- Vulnerabilities
- Policy Management
- Settings

00  
Low

000  
None

#### TOP VULNERABLE PACKAGES /

<b>linux-libc-headers 5.2</b> 325 High-risk Vulnerabilities	14	311
<b>linux-yocto 5.2.32</b> 283 High-risk Vulnerabilities	9	274
<b>python3 3.7.8</b> 21 High-risk Vulnerabilities	5	15
<b>db 5.3.28</b> 15 High-risk Vulnerabilities	1	15
<b>openssl 1.1.1g</b> 14 High-risk Vulnerabilities	1	14

#### VULNERABILITY STATISTICS /

All  CISA Only

Severity	Count
Critical	1
High	14
Medium	311
Low	15
None	274

Packageをクリックすると、そのPackageの詳細を確認することができます。

# その他の機能や操作について



Dashboard

Groups

Projects

Packages

Vulnerabilities

Policy Management

Settings

## Dashboard /

0

VULNERABLE PROJECTS



0

VULNERABLE PACKAGES



0

VULNERABILITIES



## SUMMARY /

0

Policy Violation  
Projects

0

Policy Violation  
Packages

0

Policy Violation  
CVEs

0

CISA  
CVEs

「Groups（グループ）」機能を使うと、CVEスキャン結果を他の人と共有することができます。  
スキャン結果を共有したい場合は、プロジェクトを作成する前にグループを作成ください。



Dashboard

Groups

Projects

Packages

Vulnerabilities

Policy Management

Settings

## Untitled Project /

Project Name\*

Project Description

  
0/500

Project File\*

SBOM, package details, or manifest.

[Show me how to create a sbom](#)

VIEW A SAMPLE PROJECT

Drag files here to add  
or

CHOOSE FILES

自社のLinuxのSBOMファイルをスキャンする際は、「Project Name（プロジェクト名）」を設定ください。  
SBOMファイルの作成方法は「Show me how to create a sbom」をご覧ください。  
作成したSBOMファイルをアップロードして、スキャンください。

WINDRVR