KEYSIGHT

Achieving SBOM Readiness for the EU Cyber Resilience Act (CRA)

Zahra Khani, Principal Product Manager

What is SBOM

Software Bill Of Material (SBOM) is a detailed list or inventory of all the components, both open-source and proprietary, used in a software product or application.

Each item in the SBOM provides details like the component name, version, license, and origin.

SBOMs are essential for understanding the entire software supply chain and ensuring security and compliance.

European
Cyber Resilience Act

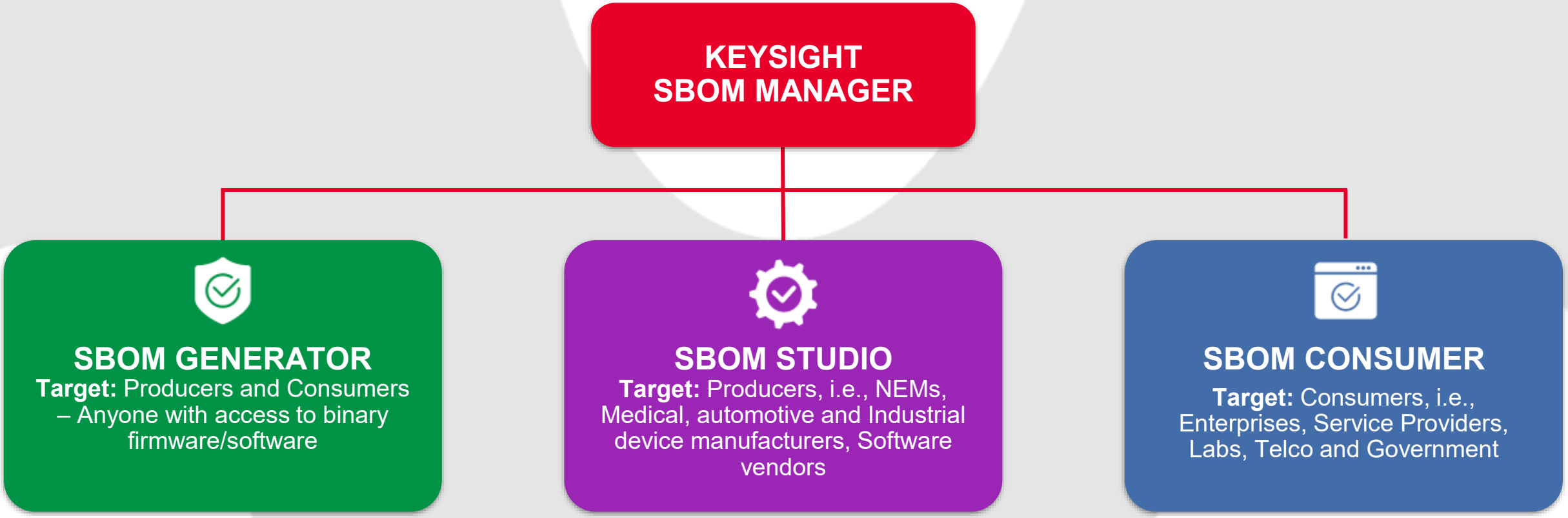
- The EU Cyber Resilience Act (CRA) establishes mandatory cybersecurity obligations for products with digital elements.
- Many of these requirements require accurate SBOM management.
- Most of these requirements come from Regulation (EU) 2024/2847, particularly Annex I – Essential Cybersecurity Requirements and Articles 13 and 14.
- Deadlines: September 2026 and December 2027

KEY REQUIREMENTS RELATED TO SBOM:

- Identify and document software components by generating a machine-readable SBOM
- Track third-party software dependencies (at least top-level components)
- Make the SBOM available to market surveillance authorities upon request
- Identify, document, monitor, and remediate vulnerabilities throughout the product lifecycle
- Report actively exploited vulnerabilities
- Do not place a new product on the market with known exploitable vulnerabilities.

KEYSIGHT

Keysight SBOM Manager



Identify and document software components by generating a machine-readable SBOM

Accuracy Matters

- The SBOM must reflect the software components in the shipped product, not just what appears in the build or development environment.
- Every declared component introduces potential liability, particularly due to vulnerability monitoring and reporting obligations.

Tooling Limitations

- Many existing SBOM tools struggle with accuracy and coverage.
- False positives introduce unnecessary liability and vulnerability management effort.
- False negatives result in missed vulnerabilities and lack of visibility into the software supply chain.

Compliance-Ready SBOMs

- SBOMs must include the minimum required elements and be delivered in machine-readable formats.
- Several frameworks could potentially be used to define minimum SBOM elements, including NTIA (2021), the CISA Draft (2025), and BSI TR-03183.
- SBOMs must include at least top-level components.
- Common formats include SPDX and CycloneDX.

Use Cases of Analyzed(Binary) SBOM

- Detects what is actually present in the shipped product and can help verify SBOM data from other sources
- Does not need access to the build process
- Provides visibility without an active development environment, such as legacy firmware artifacts
- May find hidden dependencies missed by other SBOM generation tools
- Applicable to both Device Producers and Device Consumers

KEYSIGHT

Next-Gen Binary

SBOM Detection with Keysight SBOM Generator

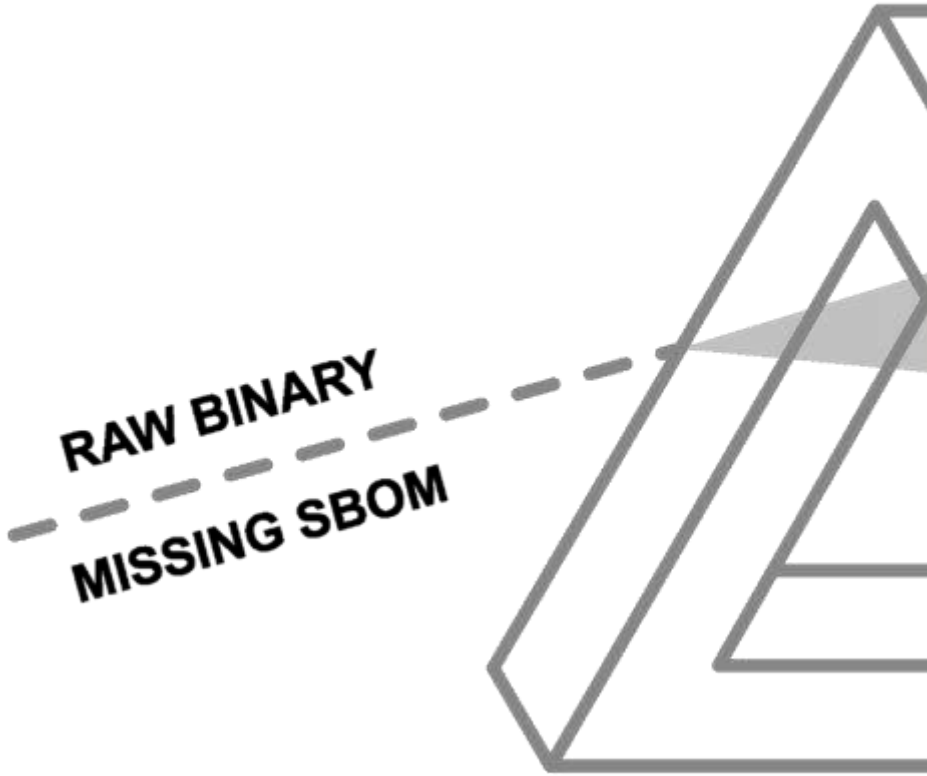
TRANSFORM YOUR BINARY BLIND SPOTS INTO ACTIONABLE SBOMS

Keysight has developed a next-generation **Analyzed SBOM** detection engine

Our binary SBOM extraction technology, goes beyond signature-based approaches

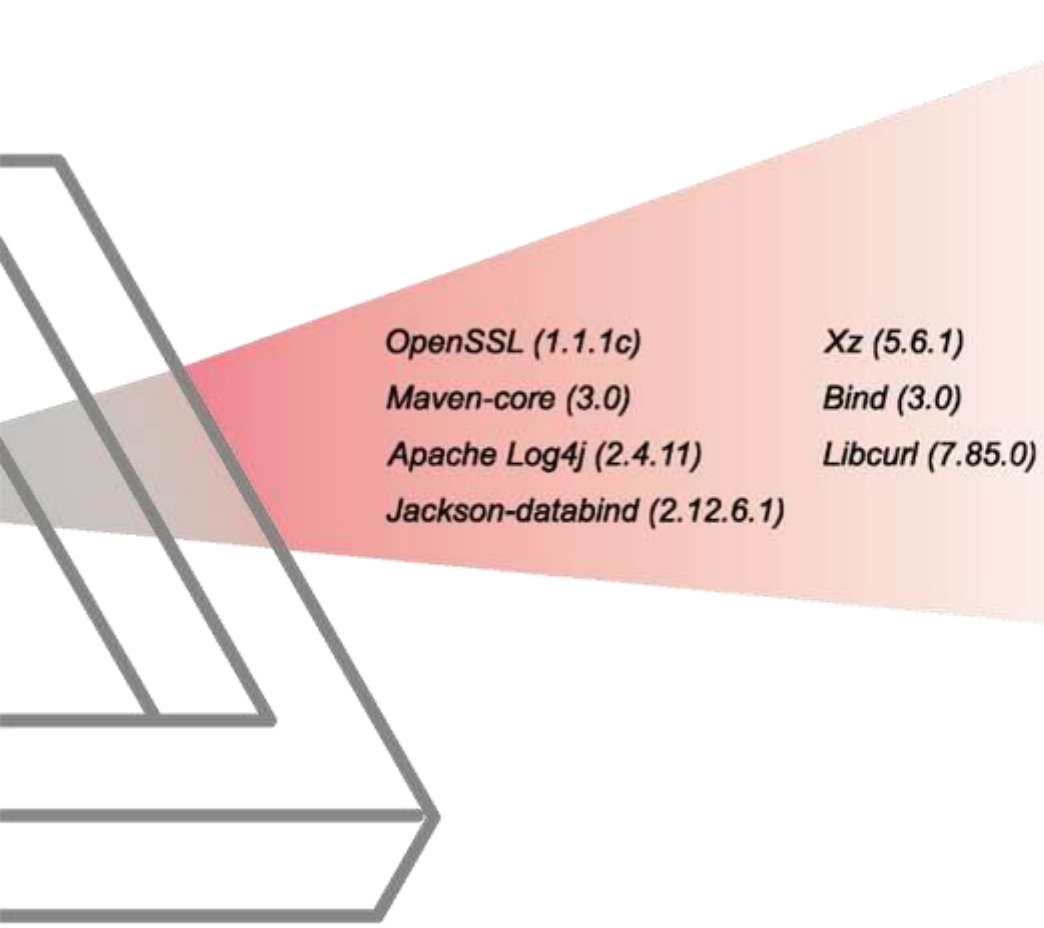
It leverages a scalable, fast, and patent-pending method based on:

- Binary similarity analysis
- Code emulation



Next-Gen Binary

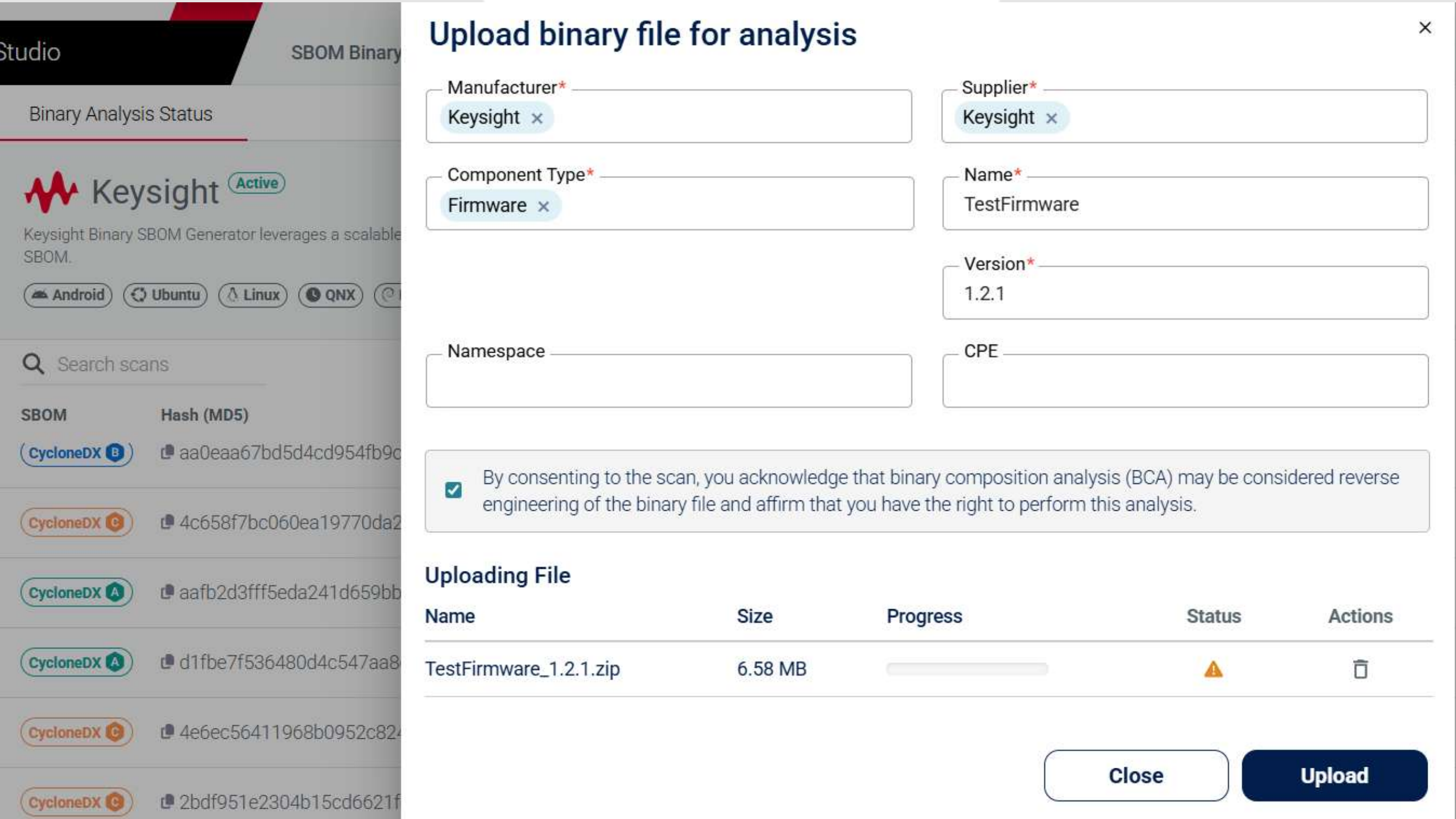
SBOM Detection with Keysight SBOM Generator



It supports detection of several open source and **closed source** components

The detection engine is highly customizable to fit your organization’s needs

Our backend infrastructure is being enhanced to support scalable component databases and future growth


Studio
SBOM Binary
Binary Analysis Status
Keysight
Active
Keysight Binary SBOM Generator leverages a scalable
SBOM.
Android
Ubuntu
Linux
QNX
Search scans
SBOM
Hash (MD5)
CycloneDX
aa0eaa67bd5d4cd954fb9c
CycloneDX
4c658f7bc060ea19770da2
CycloneDX
aafb2d3fff5eda241d659bb
CycloneDX
d1fbe7f536480d4c547aa8
CycloneDX
4e6ec56411968b0952c82
CycloneDX
2bdf951e2304b15cd6621f
Upload binary file for analysis
Manufacturer*
Keysight
Supplier*
Keysight
Component Type*
Firmware
Name*
TestFirmware
Version*
1.2.1
Namespace
CPE
By consenting to the scan, you acknowledge that binary composition analysis (BCA) may be considered reverse engineering of the binary file and affirm that you have the right to perform this analysis.
Uploading File
Name
Size
Progress
Status
Actions
TestFirmware_1.2.1.zip
6.58 MB
Close
Upload

Feb 13, 2026 32s

- Import SBOM
- Download CycloneDX
- Download CycloneDX Complete
- Weakness Report
- File cleanup status
- Archive Scan


```
        "bom-ref": "6979d09ea41d5f81e37a118d",
        "components": [
            {
                "bom-ref": "6979d0876218e9f6e962e64a",
                "hashes": [
                    {
                        "alg": "SHA-256",
                        "content": "b1dc3fea6a3a37b7545cce50b60c711e3095bced85f3459ac091170a012853aa"
                    }
                ],
                "name": "/192e36c92763486d81cd04278c70fd48.extracted/E448EC/squashfs-root/usr/bin/h2load",
                "type": "file"
            }
        ],
        "cpe": "cpe:2.3:a:nghttp2:nghttp2:1.31.1:*:*:*:*:*:*:*",
        "licenses": [
            {
                "license": {
                    "id": "MIT"
                }
            }
        ],
        "manufacturer": {
            "name": "nghttp2"
        },
        "name": "nghttp2",
        "supplier": {
            "name": "nghttp2"
        },
        "type": "library",
        "version": "1.31.1"
    },
```


- miniupnpd (2.1.20191006)
- mtd-utils (2.1.4)
- ncurses (6.3.20220423)
- ndisc6 (1.0.6)
- nettle (2.7.1)
- **nghttp2 (1.31.1)** K
- node-forge (0.10.0)
- ntfs-3g (2022.5.17)

Files (1)

Name

h2load

Types

unknown

/192e36c92763486d81cd04278c70fd48.extracted/E448EC/squashfs-root/usr/bin/h2load

b1dc3fea6a3a37b7545cce50b60c711e3095bced85f3459ac091170a012853aa

SBOM Import

SBOM Autocorrection | OSS License Autocorrection

Ignore Files | Ignore Zero Version Components

Ignore Nonexistent CPEs

Quality Analysis 2.0

General Validation	100
NTIA Minimal SBOM Elements	93
Data Validation	85

93

A

PROCESSING FILE

- File was successfully validated
- File was successfully normalized
- File was processed with warnings

General Info

SBOM Type: CycloneDX
File Format: JSON
Spec version: 1.6

Analysis Engine

Engine: keysight-sbom-generator
Vendor: Keysight

Software Details

Name: zoom
Version: 10
Type: application
Package manager: generic

SBOM Quality Analysis 2.0

COMMITTED
Jan 30, 2026 14:12:58
zahra.khani@keysight.com

PUBLISHED
Jan 30, 2026 14:13:02
zahra.khani@keysight.com

Quality Analysis	Compliance
General Validation	100
NTIA Minimal SBOM Elements	84
Data Validation	80

88

B

Quality Analysis Exception

1769782378_AL.Test1_1.1.cdx.json

CPE does not exist

Component Name	Details
shared-mime-info	Nonexistent CPE
2.1	

CPE

Close

Download

NTIA Minimal SBOM Elements

- SBOM has assembly tools
- SBOM has assembly time
- 1 of 123 components missing supplier name -4
- 1 of 123 components missing author name -4
- 123 of 123 components have name
- 38 of 123 components missing version -8
- Relationships
  - Has level 1 relationships
  - Has level 2 relationships
- Components Unique Id

SBOM Quality Analysis 2.0

COMMITTED
Jan 30, 2026 14:12:58
zahra.khani@keysight.com

PUBLISHED
Jan 30, 2026 14:13:02
zahra.khani@keysight.com

Quality Analysis | Compliance

BSI TR-03183 2.1.0 82

SBOM Creator

Details
The SBOM creator information is incomplete. Either a contact email or a URL for the manufacturer is required.

Component Creator

Component Name | Details

Close | Download

BSI TR-03183 v.2.1.0

Required

- SBOM Formats
  - compliant
- Vulnerabilities
  - compliant
- Creator of the SBOM
  - not compliant
- Timestamp
  - compliant
- Component Creator
  - 69 of 124 components are not compliant
- Component Name
  - 124 of 124 components are compliant
- Filename of the Component
  - 124 of 124 components are compliant
- Component Version
  - 2 of 124 components are not compliant
- Dependencies on Other Components
  - 124 of 124 components are compliant
- Distribution licenses
  - 124 of 124 components are not

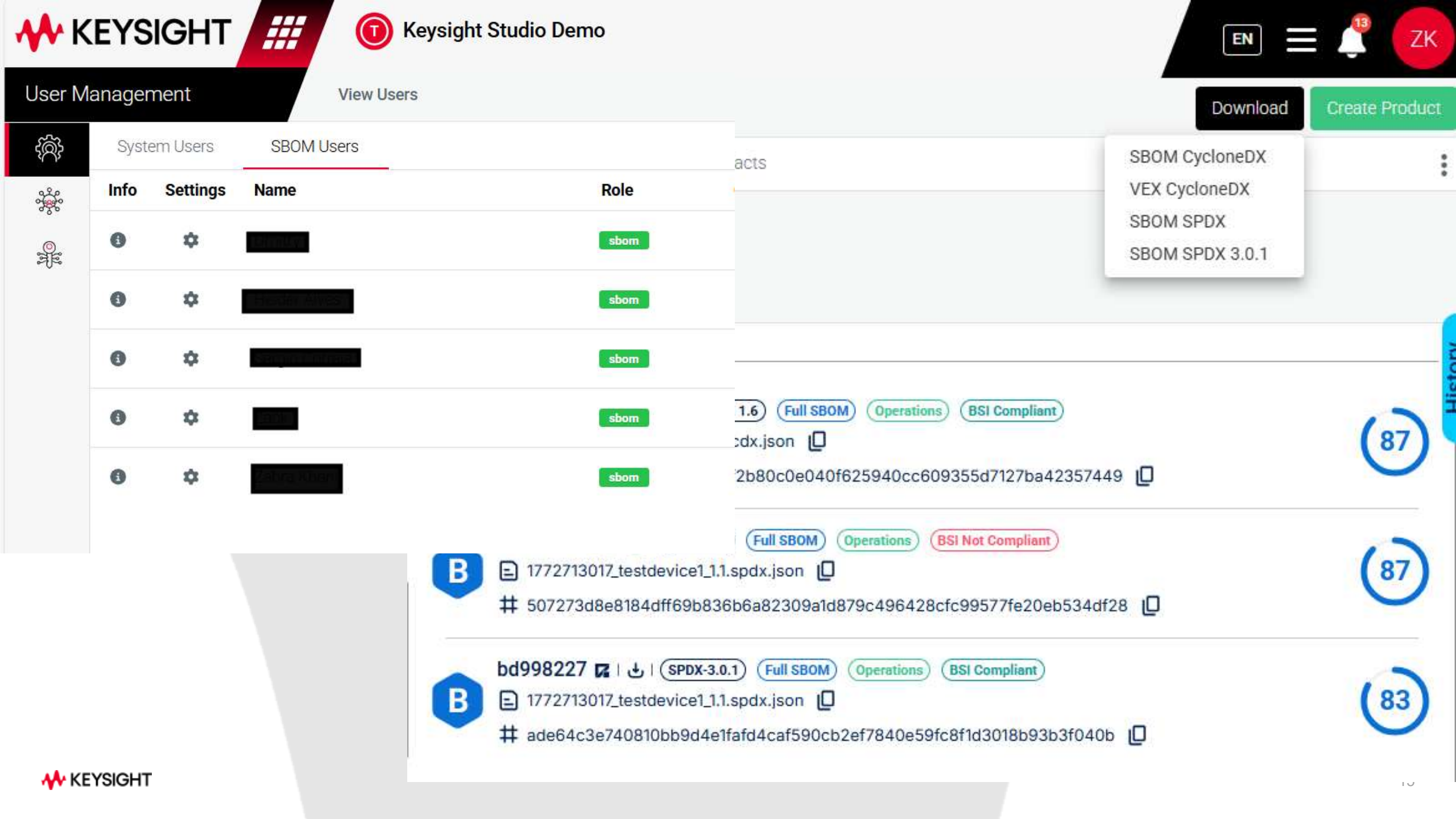
Make the SBOM available to market surveillance authorities upon request

Market surveillance authorities can use SBOMs to:

- Verify compliance with CRA software transparency requirements
- Independently analyze software components used in products
- Monitor vulnerabilities affecting those components
- Identify known or actively exploited vulnerabilities in deployed products
- Validate that manufacturers detect, report, and remediate vulnerabilities within required timelines
- They may also collaborate with organizations such as ENISA to support large-scale vulnerability monitoring and compliance tracking across products in the EU market

Manufacturers must ensure that SBOMs are:

- Accurate – Fewer false positives mean less liability
- Up-to-date for released product versions
- Available in machine-readable formats


KEYSIGHT
Keysight Studio Demo
EN
13
ZK
User Management
View Users
Download
Create Product
System Users
SBOM Users
Info
Settings
Name
Role
sbom
SBOM CycloneDX
VEX CycloneDX
SBOM SPDX
SBOM SPDX 3.0.1
1.6
Full SBOM
Operations
BSI Compliant
2b80c0e040f625940cc609355d7127ba42357449
87
Full SBOM
Operations
BSI Not Compliant
1772713017_testdevice1_1.1.spdx.json
507273d8e8184dff69b836b6a82309a1d879c496428cfc99577fe20eb534df28
87
bd998227
SPDX-3.0.1
Full SBOM
Operations
BSI Compliant
1772713017_testdevice1_1.1.spdx.json
ade64c3e740810bb9d4e1fafd4caf590cb2ef7840e59fc8f1d3018b93b3f040b
83
KEYSIGHT

Identify, document, monitor, and remediate vulnerabilities throughout the product lifecycle

Manufacturers must be able to:

- Identify vulnerabilities affecting software components used in their products including open-source projects
- Continuously monitor newly disclosed vulnerabilities impacting those components
- Document vulnerabilities and remediation actions
- Remediate vulnerabilities without undue delay, including through security updates or mitigations

Key Challenges

- Many vulnerabilities originate from third-party and open-source components embedded in firmware or software.
- Without accurate component visibility, manufacturers may miss vulnerabilities affecting their products.
- Modern products often include large software stacks (full OS images, containers, multiple software layers), resulting in large numbers of reported vulnerabilities.
- Many reported vulnerabilities may already be patched, mitigated, or not reachable in the deployed product, making impact assessment difficult and time-consuming.

Effective compliance requires:

- Accurate visibility into software components
- Accurate vulnerability correlation
- Continuous vulnerability monitoring
- Reachability analysis to determine whether vulnerabilities actually affect the product
- Clear documentation and traceability of vulnerability handling and remediation actions

Report actively exploited vulnerabilities

When reporting is required

- Manufacturers must report actively exploited vulnerabilities and severe incidents affecting product security once they become aware of them.
- “Awareness” occurs when the manufacturer has reasonable certainty after an initial assessment.

Who must be notified

- Simultaneous notification to the designated national CSIRT and European Union Agency for Cybersecurity.

Reporting timeline

- Early warning: within 24 hours of becoming aware
- Detailed notification: within 72 hours
- Final report:
  - within 14 days after mitigation is available (for exploited vulnerabilities)
  - or 1 month after the 72-hour notification (for severe incidents)

User communication

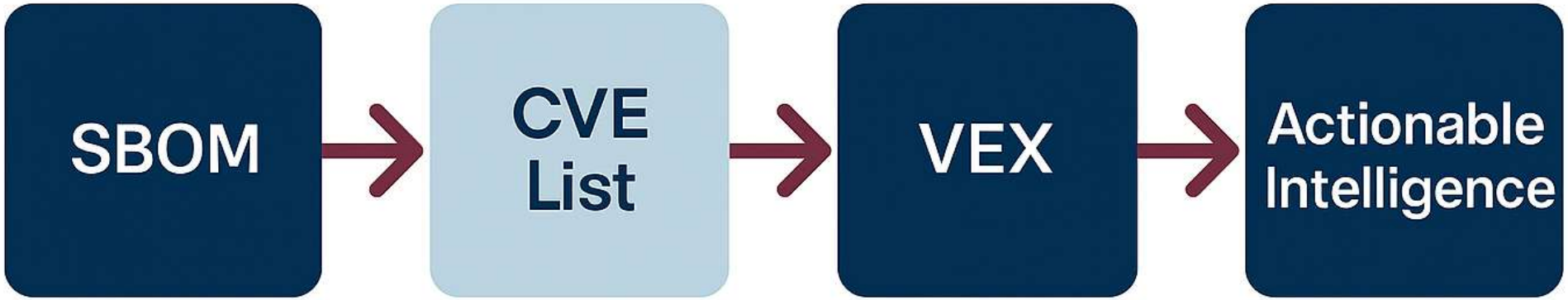
- Manufacturers must inform affected users about the vulnerability or incident.
- Disclosure should follow a risk-based approach and may initially be limited to affected users, especially for sensitive environments.

Progressive reporting

- Notifications must be updated as investigations progress and more technical details become available.

VEX

- **VEX = Vulnerability Exploitability eXchange**
- **Adds context to CVEs in SBOMs**
- **Indicates if a vulnerability is:**
  - Affected
  - Not affected – requires justification
  - Fixed
  - Under investigation
  - False Positive



for name use 'AND' / 'OR' for version use 'ver=' 'AND' / 'OR'

- libicu60 (60.2-3ubuntu3.1)
- libidn2-0 (2.0.4-1.1ubuntu0.2)
- libk5crypto3 (1.16-2ubuntu0.2)
- libkeyutils1 (1.5.9-9.2ubuntu2)
- libkrb5-26-heimdal (7.5.0+dfsg-1)
- libkrb5-3 (1.16-2ubuntu0.2)
- libkrb5support0 (1.16-2ubuntu0.2)
- libldap-2.4-2 (2.4.45+dfsg-1ubuntu1.10)
- libldap-common (2.4.45+dfsg-1ubuntu1.10)
- liblz4-1 (0.0~r131-2ubuntu3.1)
- liblzma5 (5.2.2-1.3)
- libmount1 (2.31.1-0.4ubuntu3.7)
- libncurses5 (6.1-1ubuntu1.18.04)
- libncursesw5 (6.1-1ubuntu1.18.04)
- libnettle6 (3.4.1-0ubuntu0.18.04.1)
- **libnghttp2-14 (1.30.0-1ubuntu1)** K
- libp11-kit0 (0.23.9-2ubuntu0.1)
- libpam-cap (1:2.25-1.2)
- libpam-modules (1.1.8-3.6ubuntu2.18.04.3)
- libpam-modules-bin (1.1.8-3.6ubuntu2.18.04.3)
- libpam-runtime (1.1.8-3.6ubuntu2.18.04.3)
- libpam0g (1.1.8-3.6ubuntu2.18.04.3)
- libpcre3 (2:8.39-9)
- libprocps6 (2:3.3.12-3ubuntu1.2)
- libpsl5 (0.19.1-5build1)
- libroken18-heimdal (7.5.0+dfsg-1)
- librtmp1 (2.4+20151223.gitfa8646d.1-1)
- libsasl2-2 (2.1.27~101-g0780600+dfsg-3ubuntu...
- libsasl2-modules-db (2.1.27~101-g0780600+df...
- libseccomp2 (2.5.1-1ubuntu1~18.04.1)
- libselinux1 (2.7-2build2)
- libsemanage-common (2.7-2build2)
- libsemanage1 (2.7-2build2)
- libsepol1 (2.7-1)
- libsmartcols1 (2.31.1-0.4ubuntu3.7)
- libsnappy1v5 (1.1.7-1)

Details | Vulnerabilities | Dependency Lookup | Country of Origin

libnghttp2-14 </>

1.30.0-1ubuntu1 | 4.9K | 165 | 933 | 1 / 1.4K | 44 / 1.2K | 12Y | 7M | 20D

VEXed 1/1 0/0 | Not VEXed H 2 M 1

Search vulnerabilities | Show Excluded | MultiVEX

H NVD

CVE-2023-44487

EX | 7.5 CVSS | 94% EPSS | KEV | Top 25 | Patched in: 1.30.0-1ubuntu1+esm2

Published: Oct 10, 2023 The HTTP/2 protocol allows a denial of service (server resource consumption) because request cancellation can reset many streams quic

Updated: Nov 7, 2025

VDP | VEX L2

Description

The HTTP%2F2 protocol allows a denial of service (server resource consumption) because request cancellation can reset many streams quickly, as exploited in the wild in August through October 2023.

Threat Intelligence

Summary

HTTP/2 protocol vulnerability allowing denial of service (server resource consumption) through rapid request cancellation.

VEX

L2 Zahra Khani Dec 17, 2025 14:12

Status: Not Affected
Justification: Code Not Present
Response: Workaround Available

Exploit Indicators

Source: NVD
Source Url: https://security.netapp.com/advisory/ntap-20240621-0006/

CWE-400

MITRE Top 25

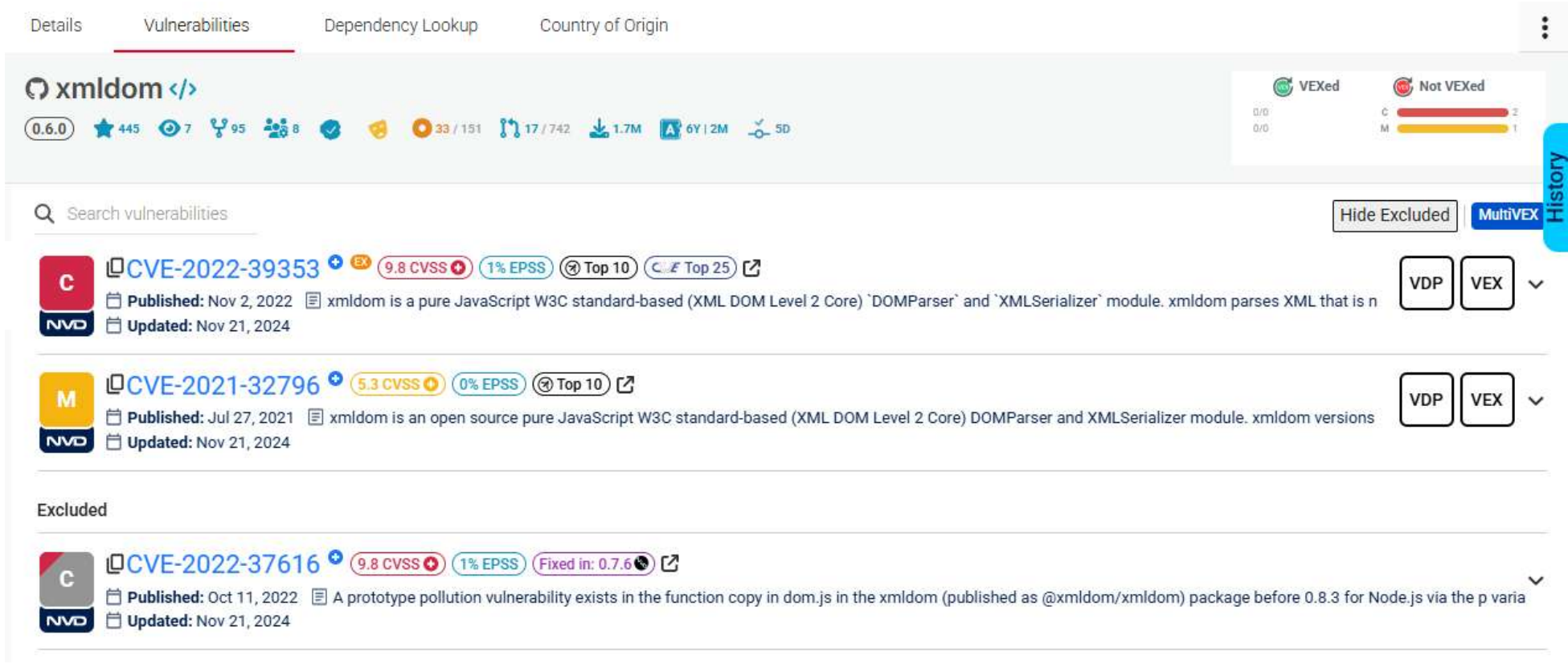
Name: Uncontrolled Resource Consumption

Known Affected Software Configurations

CPEs: cpe:2.3:a:ietf:http:2.0:*:*:*:*:*:*:*

Reducing Vulnerability False Positives and False Negatives

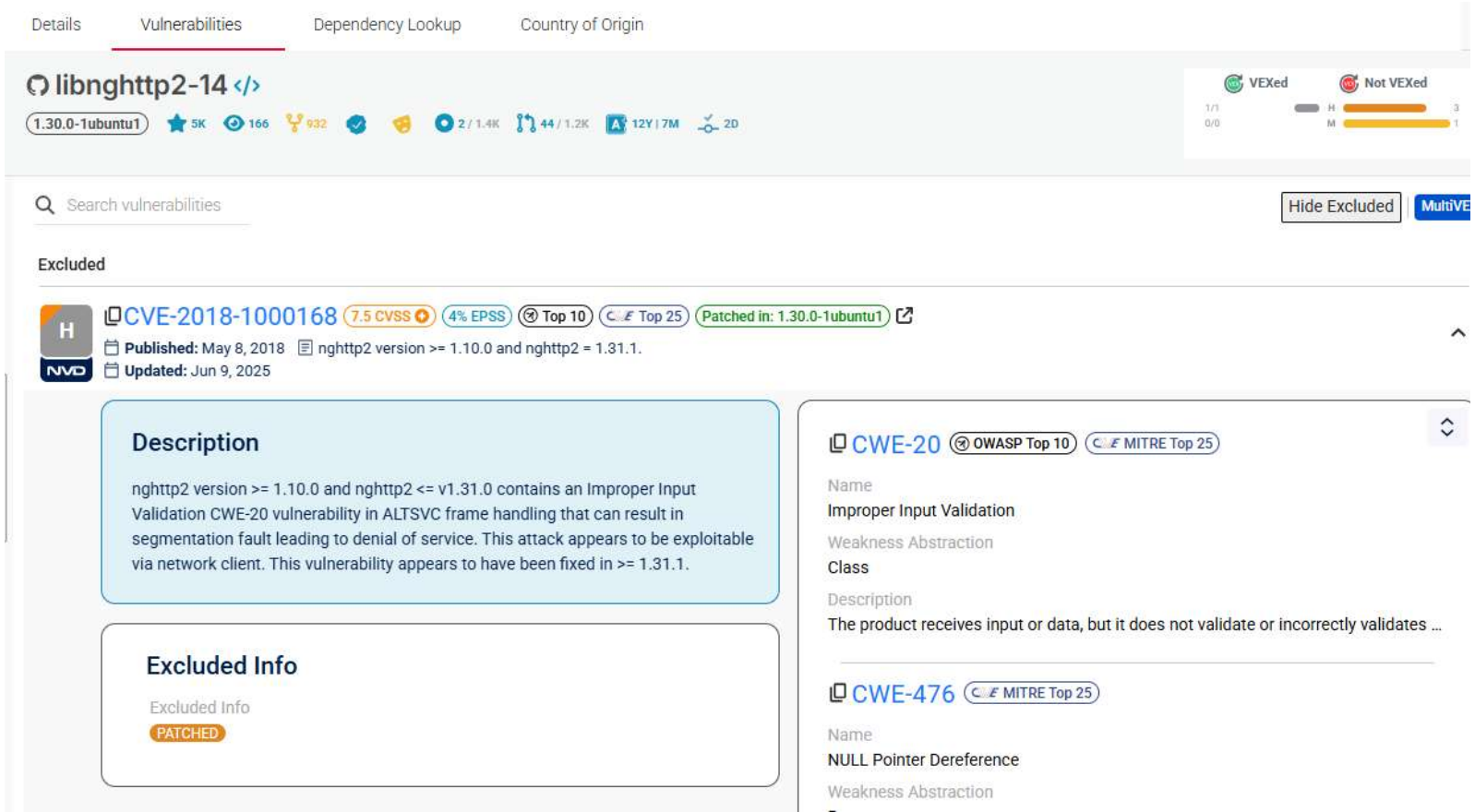
Enrich SBOM data with multiple vulnerability and threat intelligence sources and prioritizing authoritative sources whenever available instead of relying solely on the NVD.



KEYSIGHT

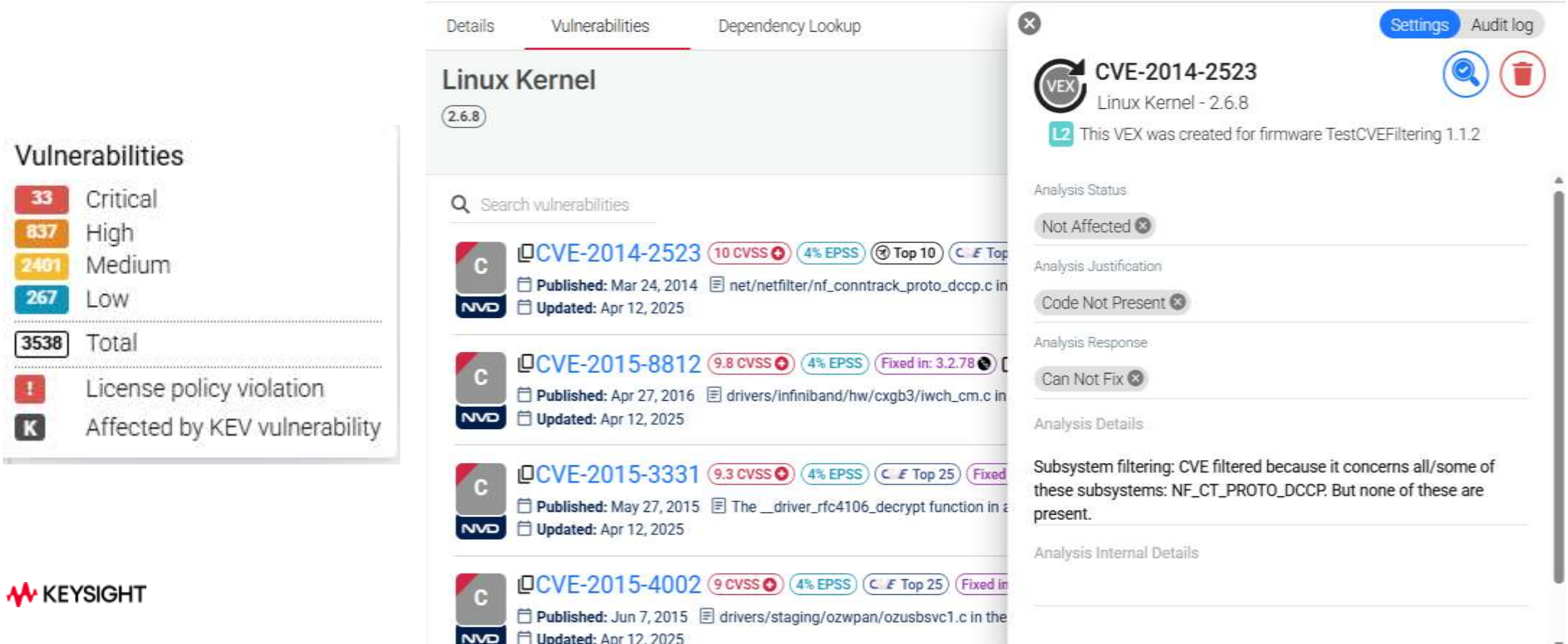
Eliminating Noise from Patched Vulnerabilities

Excluding Already Patched Vulnerabilities from the results



Advanced CVE Reachability Analysis & Automated VEX

Automatically identify unreachable CVEs and generate VEX statements, saving hundreds of hours otherwise spent evaluating vulnerability reachability and manually producing VEX.



You have 13 unread alert reports

Daily Alert: Mar 5, 2026 NEW
H CVSS EPSS

Daily Alert: Mar 4, 2026 NEW
H CVSS EPSS

Daily Alert: Mar 3, 2026 NEW
C CVSS EPSS

Daily Alert: Mar 2, 2026 NEW
H CVSS EPSS

Daily Alert: Mar 1, 2026 NEW
EPSS

Details | Dependency Lookup

CRA

Alert Option	Status	
KEV	Enabled	
KEV Due Date	Enabled	
EPSS	Enabled	5%
CVSS	Enabled	7
Severity	Enabled	High
Malicious	Enabled	

Keysight offer for EU CRA Conformity Assessment

How can we help?

Phase 1 – CRA Readiness
Product classification
Design & process review
Gap analysis
Output: Compliance plan

Phase 2 – CRA Evaluation

- Documentation review
- SBOM vulnerability verification
- Security testing & evaluation
- Output: Conformity assessment report

Product Classes and Conformity Routes

Default

Conformity to horizontal standards

Self-assessment

- CENELEC EN 40000 -2
- CENELEC EN 40000 -3
- CENELEC EN 40000 -4

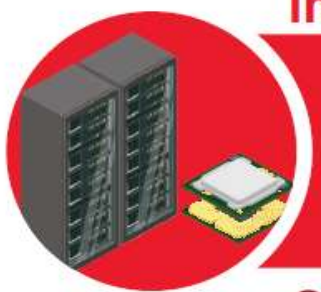
Important Class I

Conformity to vertical standards

Self-assessment

- ETSI EN 304 617-304 634

Important Class II



Module-H QA ISO 9001, ISO 17025

Third-party conformity assessment

- ETSI EN 304 635-636
- CENELEC EN 50765-50767

Critical

ISO/IEC 18045

Third-party certification

- EU Cybersecurity Certification (EUCC)

Conclusion

CRA Compliance Requires Early Preparation

- The EU CRA introduces mandatory requirements for SBOM generation, vulnerability management, and incident reporting.
- Compliance requires both technical capabilities and internal processes across the product lifecycle.

Visibility into Software Components

- Accurate SBOMs provide transparency into open-source and proprietary components within products.
- Binary analysis helps identify what is actually present in shipped software, including hidden dependencies.

From Component Lists to Risk Insight

- Enriching SBOM data with multiple vulnerability intelligence sources improves detection accuracy.
- Filtering patched vulnerabilities and identifying unreachable CVEs helps reduce false positives and prioritize real risks.

Context Matters for Vulnerability Management

- VEX adds exploitability context to vulnerabilities identified in SBOMs.
- Automated reachability analysis helps determine whether vulnerabilities are truly exploitable in your product.

Start Preparing Now

- Aligning with CRA requirements takes time and preparation across development, security, and compliance processes.
- Start building your SBOM capabilities early to meet upcoming regulatory deadlines.
- Keysight can support you at every stage with CRA readiness services, conformity assessment and certification, as well as the SBOM Manager platform to streamline SBOM generation, vulnerability analysis, and VEX management.

Thank you