

Hanwha SBOM for Supply Chain Security

September 2024

V1.0

Contents

1. The Reason of Hanwha SBOM's release

- 1.1. Supply Chain Risk
- 1.2. The rise of SBOM to address risk
- 1.3. SBOM-related legal trends

2. Introduction of Hanwha SBOM

- 2.1. The feature of Hanwha SBOM
- 2.2. How to use SBOM effectively
- 2.3. Limitations and Further challenges of Hanwha SBOM

3. Conclusion

1. The Reason of Hanwha SBOM's release

Making good use of open source to create quality products in short development cycles has become more of a necessity than an option for organizations and manufacturers.

As open source software has become a crucial portion of the software supply chain, unvalidated and unmanaged open source software components can pose a threat to organizations and their products, on both the sourcing and procuring sides of the supply chain.

This is the same situation for surveillance equipment manufacturers such as Hanwha Vision, and as the types of open source used increase and the types of products offered becomes more diverse, the need for a process that can systematically manage and track security vulnerabilities in open source software used has arisen.

1.1. Supply Chain Risk

There are two main types of risks: license risk and vulnerability risk, which are described below.

■ License risk of open source software components:

Open source software is free to use, however that does not mean it there are not any requirements that must be followed.

Open source software can be distributed under one of hundreds of licenses or without a license, so it's important to understand and comply with the obligations required by each license to reduce the risk of copyright infringement.

For example, most open source licenses require developers to provide proper copyright and license notices when copying, using, modifying, or distributing open source software.

- To ensure that proprietary software you develop does not become a derivative work of open source software, the **LGPL (GNU Lesser General Public License)** license requires dynamic linking when combined with open source software; and
- the **GPL (GNU General Public Licenses)** license requires that open source software be used as a separate work.

Thus, it is important for organizations to be aware of and comply with these varying requirements.

■ Vulnerability risk of open source software components:

In recent years, we have seen many high-profile and commonly used open source software vulnerabilities discovered, such as with Log4J, Curl, Apache Struts, and OpenSSL. This shows that it is easy for vulnerabilities to be introduced into a company or

organization's software supply chain. While it's impossible to say whether the security quality of open source software is better or worse compared to proprietary software, one thing is certain: due to the nature of open source software, where the source code is publicly available, open source vulnerabilities will continue to be reported by security professionals, acting as a self-correcting force to clean up the open source ecosystem. However, the openness of the software can also be used as a means to threaten supply chains.

1.2. The rise of SBOM to address risk

To address these risks, the importance of managing the components of incoming third-party software, especially open source software, has become critical, and the need for a management tool called the **SBOM (Software Bill Of Materials)** has arisen.

Similar to the Bill Of Materials (BOM) used in manufacturing and engineering, such as the labeling of food products for vitamins, minerals, sugars, etc., a SBOM can provide key information about its' components.

As a management tool, the SBOM must balance the licensing of open source software components with the provisioning of information about vulnerabilities and be distributed in a consistent and automated format for unified communication with various players and stakeholders in the supply chain.

For this purpose, Hanwha Vision has selected the Cyclone DX format led by the Open Web Application Security Project (OWASP, <https://owasp.org/>), an international web security standards organization, as the SBOM distribution format for this purpose and has validated it to be compliant with the Cyclone DX standard through the SBOM Utility¹.

```
Welcome to the sbom-utility! Version `v0.16.0` (sbom-utility) (windows/amd64)
=====
[ ] Loading (embedded) default schema config file: `config.json`...
[ ] Loading (embedded) default license policy file: `license.json`...
[ ] Attempting to load and unmarshal data from: `../SBOM_PNM-C16083RQZ,PNM-C32083RQZ_240722_EN_cyclonedx.json`...
[ ] Successfully unmarshalled data from: `../SBOM_PNM-C16083RQZ,PNM-C32083RQZ_240722_EN_cyclonedx.json`
[ ] Determining file's BOM format and version...
[ ] Determined BOM format, version (variant): `CycloneDX`, `1.6` (latest)
[ ] Matching BOM schema (for validation): schema/cyclonedx/1.6/bom-1.6.schema.json
[ ] Loading schema `schema/cyclonedx/1.6/bom-1.6.schema.json`...
[ ] Schema `schema/cyclonedx/1.6/bom-1.6.schema.json` loaded.
[ ] Validating `../SBOM_PNM-C16083RQZ,PNM-C32083RQZ_240722_EN_cyclonedx.json`...
[ ] BOM valid against JSON schema: `true`
```

[Figure 1] Validation check for Cyclone DX format

The SBOM Utility has been selected to avoid consistency issues that can undermine the effectiveness of the SBOM as an automation management tool, as it is crucial to ensure compatibility and compliance with the SBOM standards.

1.3. SBOM-related legal trends

Many companies and government organizations are emphasizing the need for and importance of a SBOM as a part of software supply chain management to ensure the security and quality of software.

¹ "sbom-utility" can be downloaded at <https://github.com/cyclonedx/sbom-utility>

Furthermore, legislation and regulations are being developed in many countries to mandate or encourage the use of a SBOM, including the European Union's Cyber Resilience Act, the Biden Administration's Executive Order on Improving National Cybersecurity (EO-14028), the FDA's cyber device regulations, and PCI-DSS 4.0. The Table below includes an overview of each legislation and regulation, the field impacted, and implementation timelines.

Accordingly, Hanwha also decided that it is necessary to join the trend of SBOM distribution.

[Table 1] The SBOM Regulatory Compliance Landscape²

Legislation and regulation	Who	What	When
EO 14028	Suppliers selling to the U.S. federal government; Software released or updated after September 14, 2022	Submit self-attestation form affirming compliance, and provide SBOM if requested	6/11/24 for Critical Infrastructure and 9/11/24 for all others
Cyber Resilience Act	Manufacturers of digital products selling in EU	Provide top-level SBOM	36 months after publication, which is expected in the spring or summer of 2024 (although vulnerability reporting requirements will take effect sooner)
FDA	Medical device manufacturers going through the premarket submission process for cyber devices	NTIA-compliant SBOM, plus support information for all components and a vulnerability assessment (that includes controls and/or mitigation steps)	Requirements applies to submission on or after 3/29/2023. FDA was given "refuse to accept" authority on 10/1/23

² This table was prepared with reference to <https://fossa.com/learn/sboms#the-sbom-regulatory-compliance-landscape>



PCI-DSS	Payment software providers; any software that is part of the CDE (Cardholder Data Environment) or has the potential to negatively affect the CDE	Inventory of all custom-developed and third-party software components in scope	3/31/25 for mandatory enforcement
---------	--	--	-----------------------------------

2. Introduction of Hanwha Vision's SBOM

2.1. Features of Hanwha Vision's SBOM

Hanwha Vision also decided to specify and manage the information that is essential to a SBOM including the name and version of open source software components, their source, functional description, license, copyright holder, Common Platform Enumeration (CPE), Package URL (purl), & vulnerability patch information.

■ Information provided by SBOM

- ✓ Name (components > name)

```
name: "lighttpd"
```

- ✓ Version (components > version)

```
version: "1.4.53"
```

- ✓ Source url (components > supplier > url)

```
supplier:  
  url:  
    0: "https://www.lighttpd.net"
```

- ✓ Functional description (components > description)

```
description: "lighttpd (pronounced /lighty/) is a secure, fast, compliant, and very flexible web server that has been optimized for high-performance environments. lighttpd uses memory and CPU efficiently and has lower resource use than other popular web servers. Its advanced feature-set (FastCGI, CGI, Auth, Output-Compression, URL-Rewriting and much more) make lighttpd the perfect web server for all systems, small and large."
```

- ✓ License (components > licenses > license > name)

```
licenses:  
  0:  
    license:  
      name: "BSD 3-clause License"
```

- ✓ Copyright holder (components > copyright)

```
copyright: "Copyright (c) 1991-1992, RSA Data Security, Inc.\nCopyright (c) 1995-1996 Open Market, Inc.\nCopyright (c) 2010, Norio Kobota\nCopyright (c) 2017, Glenn Strauss\nCopyright (c) 2004, Jan Kneschke, incremental "
```

- ✓ CPE [Common Platform Enumeration] (components > cpe)

[※ provide only if exists]

```
cpe: "cpe:2.3:a:lighttpd:lighttpd:1.4.53:*:*:*:*:*:*"
```

- ✓ Purl [Package Uniform Resource Locators] (components > purl)

[※ provide only if exists]

```
purl: "pkg:deb/debian/lighttpd@1.4.53-4%2Bdeb10u1"
```

- ✓ Vulnerability patch (components > pedigree > patches) [※ provide only if exists]

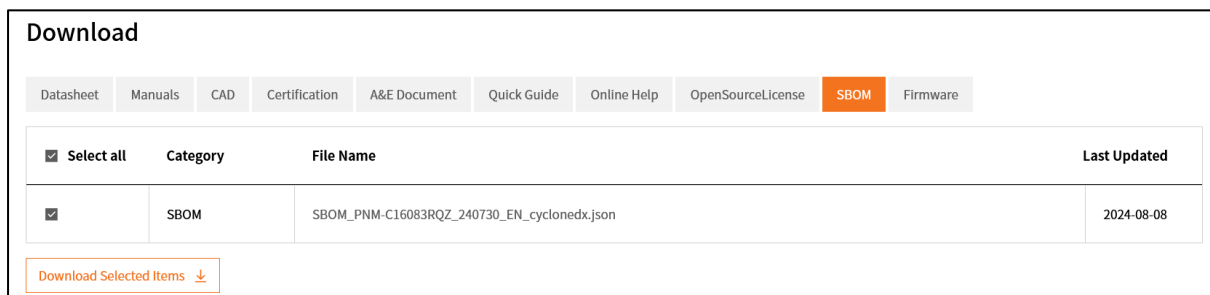
```

pedigree:
  patches:
    0:
      type: "cherry-pick"
      resolves:
        0:
          type: "security"
          id: "CVE-2022-46908"
          name: "CVE-2022-46908"
          source:
            name: "National Vulnerability Database"
            url: "https://nvd.nist.gov/vuln/detail/CVE-2022-46908"

```

2.2. How to use a SBOM effectively

The SBOM can be downloaded as shown below on the download page for each product on the Hanwha Vision website³.




[Figure 2] SBOM download location

The SBOM plays a vital role in increasing software transparency and enables customers to make informed decisions about the software they use. Therefore, customers can use the information about the software mentioned in the SBOM provided by the manufacturer to determine product vulnerabilities and take follow-up actions as follows:

■ Customer usage scenarios for SBOM:

1. A customer wants to determine if their product is impacted by a Known CVE (Common Vulnerabilities and Exposures) in a particular piece of open source software. Without having to contact the vendor, they can browse the vendor-distributed product-specific SBOM to find out which open source software is affected by the vulnerability. They can

³ Hanwha Vision website - <https://www.hanwhavision.com>



then determine if they are using the open source software and version affected by the vulnerability.

2. If you are affected, check to see if a vulnerability patch (pedigree information in SBOM) exists for the vulnerability. Sometimes a security CVE is backported to older versions, indicated that you are not vulnerable.

3. If a vulnerability patch does not exist in the SBOM, the vulnerability-related code is either not included by the compiler at build time, or because there may be cases where the vulnerability is not exposed to the outside world, and you should contact the manufacturer to determine if the vulnerability actually affects their product.

If there is an actual impact, you can ask the manufacturer to update or patch the open source software. However, if it is a discontinued model, support will be determined by whether or not the Long-Term Firmware Support Policy applies and for what period.

[For more information, see the [Long-Term Firmware Support Policy](#) document].

■ Introduction of manufacturer response process for SBOM:

1. Hanwha identifies the open source software used for each product and lists it in the SBOM.

2. Hanwha regularly monitors and evaluates the vulnerabilities of the open source software listed in the SBOM to identify risks.

3. For identified risks, we determine the risk level of the vulnerability from the perspective of customer impact and the likelihood of an attack on the product utilizing the vulnerability.

4. Risks that are determined to be impactful are addressed by releasing improved firmware in the form of version updates or patches to open source software, or by providing ways to eliminate the possibility of an attack, such as mitigating the risk by releasing security guides that show how to eliminate possible attacks.

2.3. Limitations and Further challenges of a SBOM

While any SBOM can have limitations, Hanwha Vision will work with its' customers to solve the problems of software supply chain management as well as working to resolve security vulnerabilities inherent in products in a transparent and proactive manner.

■ Challenges to distributing a SBOMs for Hanwha Vision products:

Deployment will be starting with firmware version v24.00.00.

※ Products with firmware versions prior to v24.00.00 are not eligible for SBOM distribution.

■ Two sides of the SBOM:

Pro: Provides customers with transparency into software components and enables manufacturers to be proactive about open source vulnerabilities.

Cons: Malicious actors can exploit publicly available information about software components in their attacks as well as to target specific devices due to disclosed information. Information about open source vulnerabilities provided through CPE is not complete, so there is the potential for misinformation to misdiagnose a device as being vulnerable (false positive).

■ Limitations and further plans for SBOM at Hanwha Vision:

Please note that the SBOM only contains information about open source software. Any proprietary software is excluded from these disclosures.

In addition, the current version of the SBOM does not include dependency information. We are planning to provide additional information including dependency and expanding for additional models in the future.

■ The importance of ongoing security activities to enhance product security:

Open source vulnerabilities present in a product are only one factor in assessing product vulnerabilities and cybersecurity, not all, so it is important to perform a vulnerability assessment on the actual product while considering open source vulnerabilities.

In other words, while open source updates or patches are important, it's more important to evaluate whether the open source vulnerability is manifesting itself from a product perspective in the real world.



3. Conclusion

When considering product cybersecurity in relation to open source vulnerabilities, it is important to note that the majority of these vulnerabilities are not exploitable or accessible to the real world. However, some open source vulnerabilities in the supply chain can be very threatening, and there is a growing consensus across industries and many countries about the need for management and visibility of these risks.

However, when a new high-risk vulnerability is publicly disclosed, you can now search the SBOM to determine if the product includes an affected version of the open source component.

Hanwha Vision is not satisfied with simply distributing a SBOM, as we will also work to eliminate risks from known vulnerabilities in open source software components through regular firmware updates as per a product's Long Term Firmware Support Policy.

Hanwha Vision will continue to conduct penetration tests to find product vulnerabilities, bug bounty programs for internal developers, security checks, and security reviews and remain faithful to its given role as a CNA (CVE Numbering Authority), and a leader in world class video surveillance manufacturing with its' supply chain of trust and continual focus on cybersecurity.

Hanwha Vision Co., Ltd.
13488 Hanwha Vision R&D Center,
6 Pangyo-ro 319-gil, Bundang-gu, Seongnam-si, Gyeonggi-do
TEL 070.7147.8771-8
FAX 031.8018.3715
www.HanwhaVision.com

Copyright © 2024 Hanwha Vision Co., Ltd. All rights reserved.

