

HUAWEI TECHNOLOGIES CO., LTD.
Huawei Industrial Base
Bantian Longgang
Shenzhen 518129, P.R. China
Tel: +86-755-28780808
<https://e.huawei.com/en/products/storage>



Huawei Vulnerability Management White Paper



Copyright©Huawei Technologies Co., Ltd. 2023. All rights reserved.

No part of this document may be reproduced or transmitted in any form or by any means without prior written consent of Huawei Technologies Co., Ltd.

Trademark Notice

 , HUAWEI, and  are trademarks or registered trademarks of Huawei Technologies Co., Ltd.
Other trademarks, product, service and company names mentioned are the property of their respective owners.

General Disclaimer

The information in this document may contain predictive statements including, without limitation, statements regarding the future financial and operating results, future product portfolio, new technology, etc. There are a number of factors that could cause actual results and developments to differ materially from those expressed or implied in the predictive statements. Therefore, such information is provided for reference purpose only and constitutes neither an offer nor an acceptance. Huawei may change the information at any time without notice



Contents

1 Introduction 03

2 Vulnerability Management Is Crucial to Cyberspace Security 03

3 Vulnerability Management Is the Industry's Shared Responsibility and Requires Collaboration 04

4 Huawei Establishes Its Vulnerability Management System and Develops Engineering Capabilities in Line with Industry Standards and Best Practices 05

4.1 Huawei's Vulnerability Management Concepts 05

4.1.1 Vulnerability Management Objectives 05

4.1.2 Vulnerability Management Principles 06

4.1.3 Key Phases of Vulnerability Handling 06

4.1.4 Codes of Conduct for Vulnerability Management 07

4.2 Huawei Vulnerability Management Framework and Practice 08

4.2.1 Full-View Vulnerability Management 09

4.2.2 Vulnerability Management Throughout Product Lifecycle 09

4.2.3 Supply Chain Management 11

4.2.4 Vulnerability Management Platform 12

5 Summary 13



1 Introduction

The rapid development and application of big data, industrial Internet, cloud computing, artificial intelligence, and other new technologies are driving advancements in businesses' digital services, leading to a prosperous digital economy. However, these new technologies also contribute to the increasing complexity of software architectures and the emergence of new attack methods. As a result, businesses' service systems are exposed to more security vulnerabilities.

In the context of frequent cybersecurity incidents, businesses are increasingly aware of cybersecurity risks, and vulnerability management has become an important part of their cybersecurity strategies. Additionally, different countries and regions have legislated to manage cybersecurity vulnerabilities.

2 Vulnerability Management Is Crucial to Cyberspace Security

Over the past few years, the number of cyberspace security threats has shot up dramatically. Such threats — which can cause major losses — include cyber ransomware and supply chain security incidents. Vulnerability exploitation remains one of the main causes of security incidents. Building end-to-end supply chain vulnerability management throughout the product lifecycle is an important means to reduce risks on live networks and ensure service continuity.

As the digital transformation of industries around the world deepens, cybersecurity attacks are becoming more and more frequent and automated. The presence of high-risk vulnerabilities and security incidents has given rise to the need for legislation and supervision as well as related technology development. China, the UK, Europe, and the US have released laws and regulations to coordinate vulnerability management, recognizing its significance in national cybersecurity strategies.

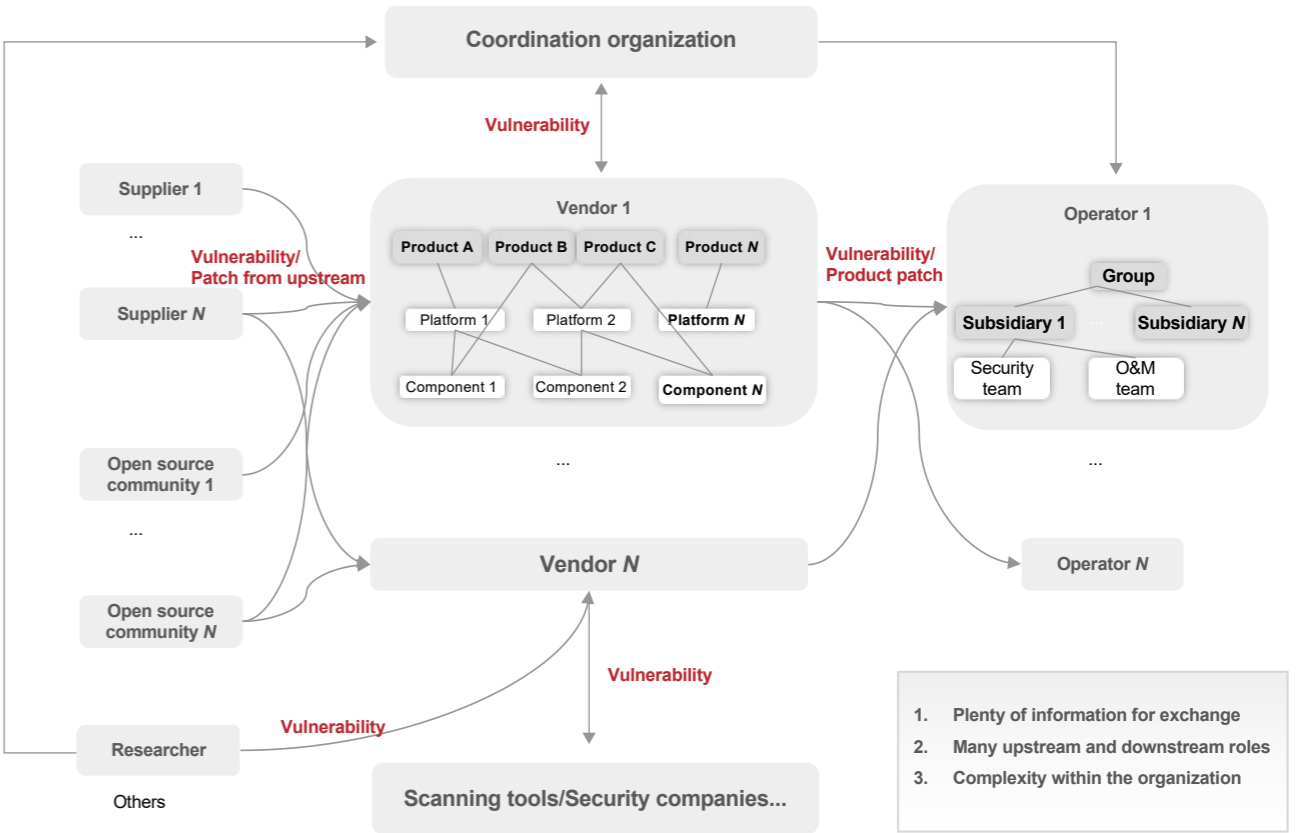
The maturity of businesses' vulnerability management directly reflects their digital governance levels and software engineering capabilities — it is also closely linked to sustainable business development. Businesses must collaborate with stakeholders to continuously manage vulnerabilities. Failure to do so may result in system breakdown, information leakage, and other risks, compromising business assets and reputation and even hindering businesses' long-term development.

3 Vulnerability Management Is the Industry's Shared Responsibility and Requires Collaboration

Vulnerability management involves multiple stakeholders across the entire supply chain, for example, suppliers (including open source communities), equipment vendors, carriers, and consumers. It includes vulnerability awareness, verification, remediation, disclosure, and live-network vulnerability risk mitigation throughout the product lifecycle. Ensuring prompt, accurate, and secure exchange of vulnerability information among stakeholders, however, is an industry-wide challenge. The complexity of vulnerability management is further aggravated by large-scale collaborative development of modern software, including software products, platforms, and components, within businesses.

Vulnerability management requires upstream and downstream collaboration to ensure that all involved parties fulfill their vulnerability management responsibilities. This is to establish a continuous relationship of trust and cooperation throughout the entire supply chain in an open and cooperative manner, enhance trust and capabilities, and collectively mitigate cybersecurity risks arising from vulnerabilities.

Figure 3-1 Collaboration in vulnerability management

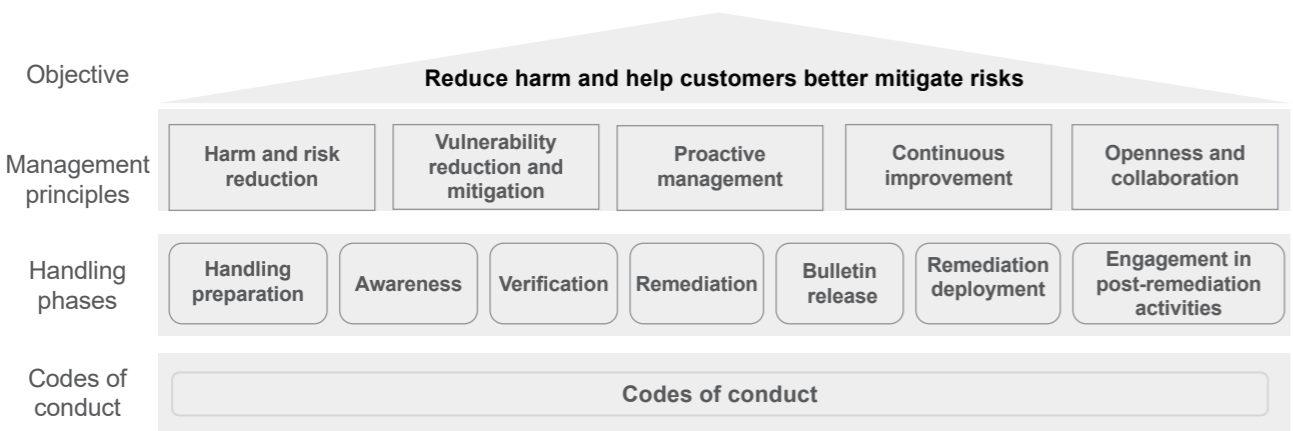


4 Huawei Establishes Its Vulnerability Management System and Develops Engineering Capabilities in Line with Industry Standards and Best Practices

4.1 Huawei's Vulnerability Management Concepts

Huawei regards an end-to-end global cybersecurity assurance system as one of its development strategies. It has established a sustainable and trusted vulnerability management system in terms of policies, organizations, processes, technologies, and specifications, and collaborates with external stakeholders to address vulnerability challenges together. Huawei proposes five basic principles for vulnerability management and specifies seven vulnerability handling phases and corresponding codes of conduct to guide business departments in vulnerability management activities.

Figure 4-1 Huawei vulnerability management architecture



4.1.1 Vulnerability Management Objectives

To better support the mitigation of vulnerability risks on customers' live networks, Huawei has divided vulnerability management objectives into three aspects:

1. Responsible disclosure: Establish a vulnerability disclosure and communication mechanism with customers who purchase Huawei products and solutions to support customers' decision-making on vulnerability risks.
2. Vulnerability reduction and mitigation: Establish a full-view and end-to-end vulnerability management mechanism throughout the product lifecycle to rapidly detect, investigate, mitigate, and fix vulnerabilities and support customers in risk mitigation.
3. Collaborative management: Specify a collaboration mechanism with suppliers and cus-

tomers to mitigate vulnerability risks.

4.1.2 Vulnerability Management Principles

1. Harm and risk reduction

Our vision for vulnerability management is to reduce the harm and security risks caused by vulnerabilities in Huawei products and services to customers/users. This vision guides us when handling and disclosing vulnerabilities.

2. Vulnerability reduction and mitigation

The industry recognizes that vulnerabilities are inevitable^{[1][2][3]}, but we strive to: (1) Take measures to reduce vulnerabilities in products and services. (2) Promptly provide risk mitigations for customers/users once vulnerabilities in products and services are found.

3. Proactive management

Vulnerability issues need to be resolved through upstream and downstream collaboration in the supply chain. We proactively identify and fulfill our responsibilities in vulnerability management and build our management system based on laws, regulations, contracts, and open standards to proactively manage vulnerabilities.

4. Continuous improvement

Cybersecurity is a constantly evolving process where threats and attacks also evolve constantly. As such, defense must be adapted accordingly. We will continue to learn from industry standards and best practices in order to drive the maturity of our vulnerability management.

5. Openness and collaboration

We will continue to adopt an open and cooperative attitude and strengthen the connection with the supply chain and external security ecosystem. And we will enhance collaboration with stakeholders to build trusted cooperation relationships.

4.1.3 Key Phases of Vulnerability Handling

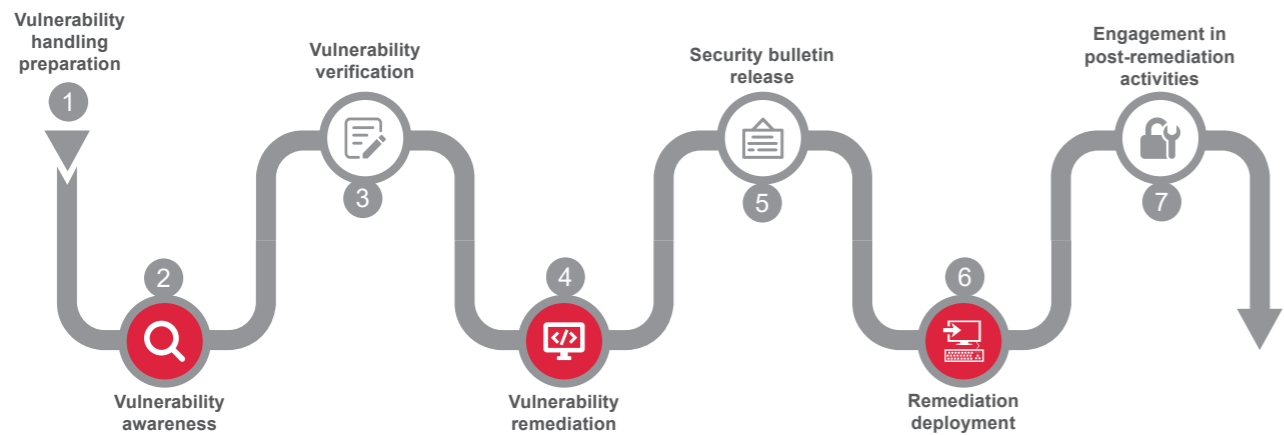
Huawei is committed to enhancing the security of its products and solutions in order to fully support the secure operations of customers' networks and services. In accordance with ISO/IEC 30111 and ISO/IEC 29147, Huawei has developed a comprehensive vulnerability handling process to safeguard product security. And to jointly address vulnerability risks and challenges, it has also established an open, collaborative ecosystem.

¹ <https://www.tenable.com/blog/vulnerabilities-in-cybersecurity-how-to-reduce-your-risk>

² https://www.ntia.gov/files/ntia/je_savage_05182015.pdf

³ <https://www.secpoint.com/vulnerabilities-are-unavoidable.html>

Figure 4-2 Seven key phases of vulnerability handling



- 1.Vulnerability handling preparation: Build policies, organizations, and capabilities for vulnerability disclosure and handling.
- 2.Vulnerability awareness: Establish vulnerability awareness channels to receive reports about suspected vulnerabilities.
- 3.Vulnerability verification: Confirm the validity and impact scope of suspected vulnerabilities.
- 4.Vulnerability remediation: Develop and implement vulnerability remediations.
- 5.Security bulletin release: Release vulnerability remediation information to customers.
- 6.Remediation deployment: After receiving the vulnerability remediation information, operators assess risks and deploy remediations on their live networks to mitigate risks.
- 7.Engagement in post-remediation activities: Make continuous improvement based on customer comments and internal practices.

4.1.4 Codes of Conduct for Vulnerability Management

To guide business departments more effectively in terms of vulnerability management activities, Huawei proposes the codes of conduct for key activities in the vulnerability handling process:

- 1.In the vulnerability handling preparation phase, establish vulnerability handling organizations and processes, specify handling objectives, and establish external communication channels.
- 2.In the vulnerability awareness phase, establish extensive internal and external channels to collect all vulnerability information related to Huawei products, in order to verify and fix vulnerabilities promptly.
- 3.In the vulnerability verification phase, verify the impact of perceived vulnerabilities on

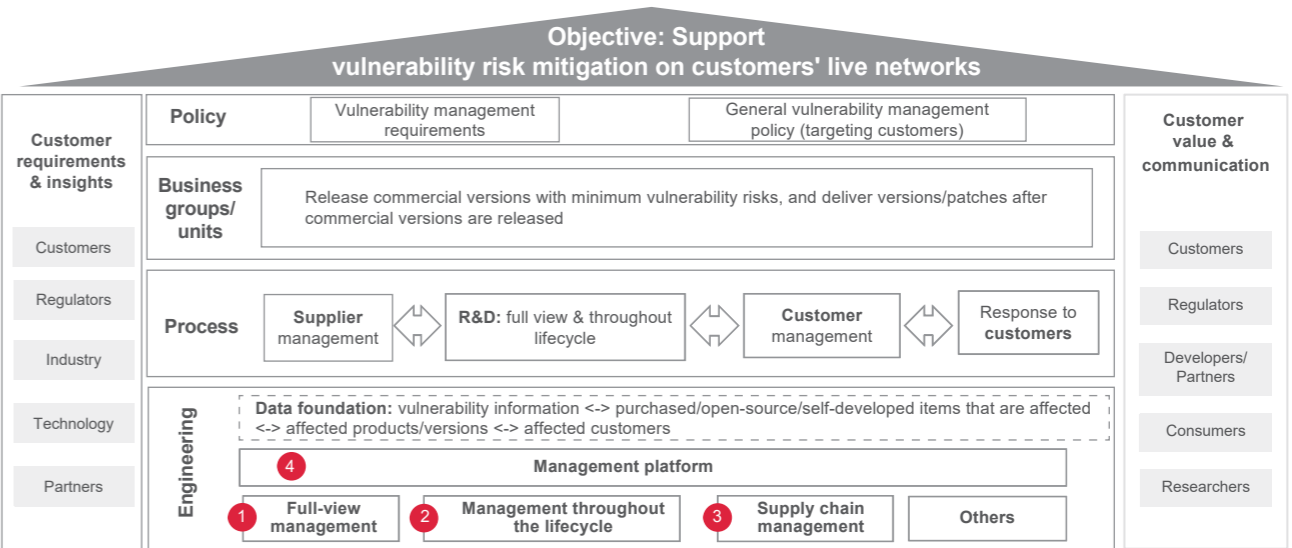
product versions within the lifecycle, and maintain continuous and clear communication with vulnerability reporters.

- 4.In the vulnerability remediation phase, take proactive actions to mitigate and fix vulnerabilities. In addition, address all vulnerabilities based on their severity and other factors to ensure that they are properly handled.
- 5.In the security bulletin release phase, disclose vulnerability information only to affected stakeholders, through proper internal and external collaboration.
- 6.In the remediation deployment phase, deploy or help customers deploy remediations, proactively communicate with customers about high-risk vulnerabilities, and encourage customers to actively manage patches and stay updated on security bulletins so that they can detect and mitigate vulnerabilities promptly.
- 7.During engagement in post-remediation activities, product teams should analyze the root causes of vulnerabilities to improve security activities. In addition, product teams should continuously foster and raise security awareness and capabilities among all employees through external communication and through collaboration between upstream and downstream stakeholders in the industry chain.

4.2 Huawei Vulnerability Management Framework and Practice

To help customers mitigate vulnerability risks on live networks, Huawei has established a vulnerability management framework, including policies, processes, engineering, culture, and organizations. Furthermore, it has continued to improve its capabilities in each business group/unit to support efficient and well-organized vulnerability management.

Figure 4-3 Huawei vulnerability management framework



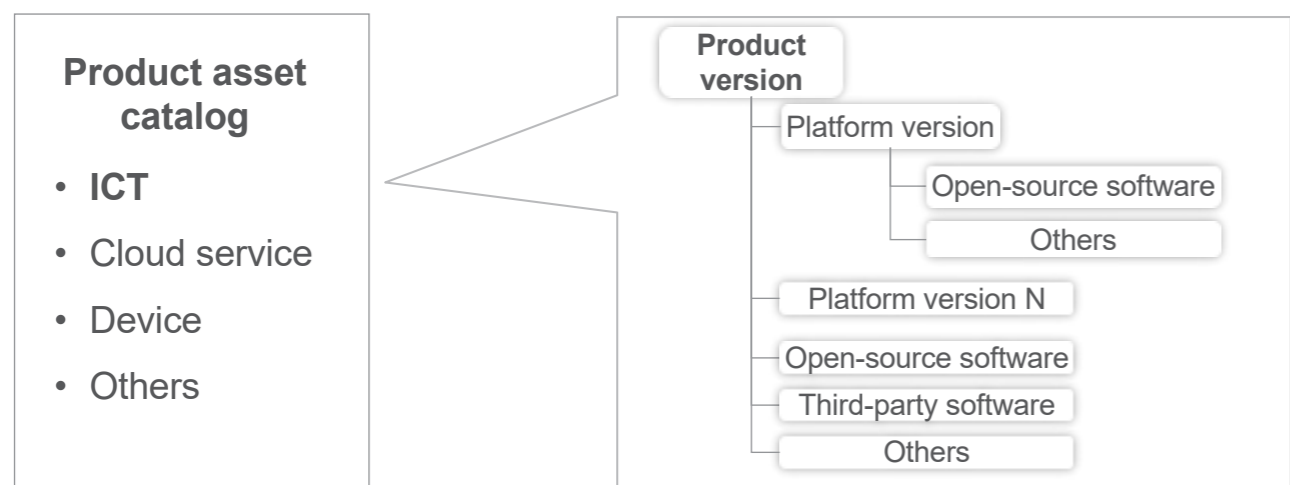
4.2.1 Full-View Vulnerability Management

Asset management is the basis of vulnerability management, yet it is an industry-wide challenge to ensure the integrity and accuracy of asset information. Furthermore, Huawei operates in multiple business groups/units, including ICT, cloud service, device, and Intelligent Automotive Solution (IAS), and each one encompasses different types of assets. Therefore, it is challenging to produce a comprehensive and up-to-date list of assets. In addition, identifying precise information about open-source and third-party software in assets is a common industry challenge.

Huawei has assigned business directors of business groups/units as primary owners for vulnerability management. When a product charter is initiated, assets must be registered to ensure that the asset list is managed from the very beginning. During development, software engineering capabilities (such as full source code build) are set up to ensure that the sources of assets in use (including platforms, open-source software, and third-party software) are managed.

A full picture of vulnerabilities in product versions can be drawn based on all available software asset information. This is helpful for vulnerability verification, remediation, and other management activities.

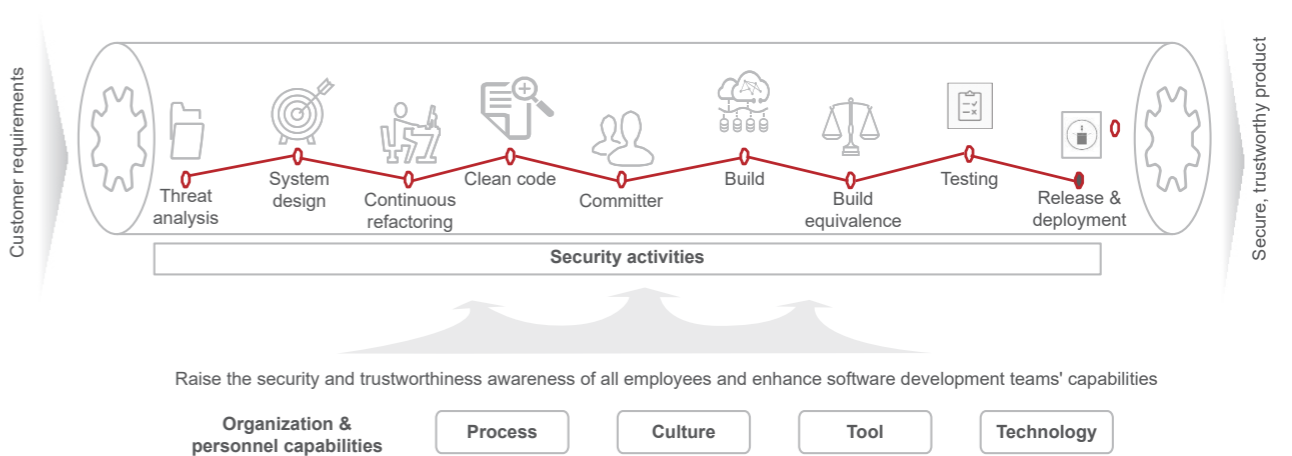
Figure 4-4 Full-view vulnerability management



4.2.2 Vulnerability Management Throughout Product Lifecycle

Huawei adheres to the concept of "building security in design, processes, and operations" throughout the product lifecycle. It has established processes to ensure that cybersecurity assurance measures are effectively implemented in each phase to improve product security competitiveness.

Figure 4-5 IPD process with built-in cybersecurity

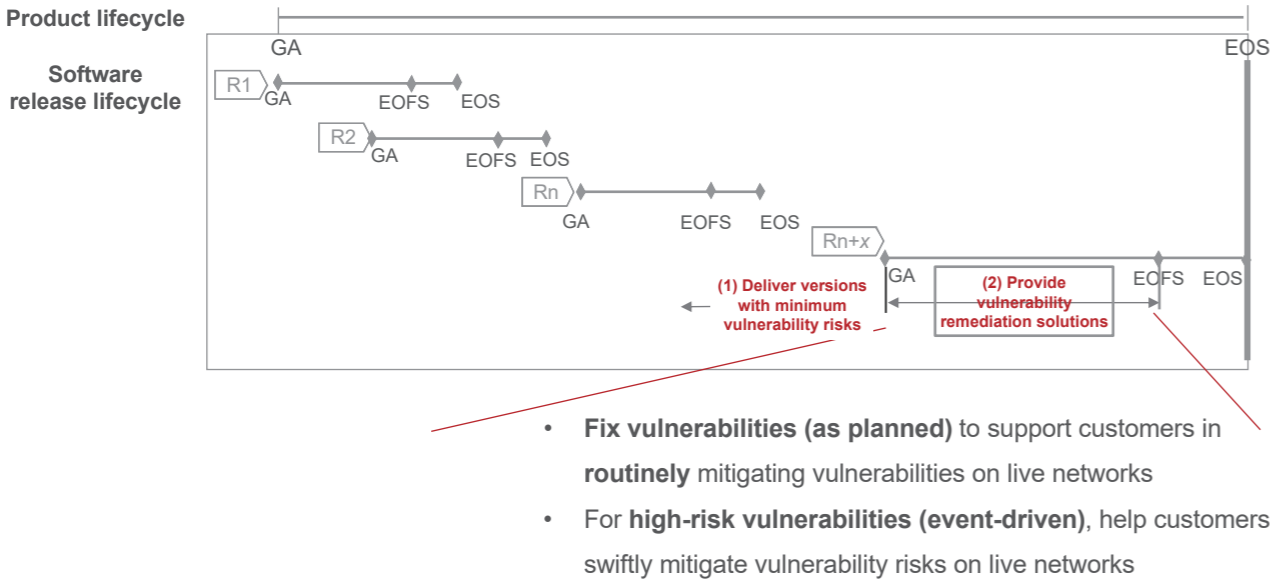


The Integrated Product Development (IPD) process includes the concept, plan, develop, qualify, and launch phases. Threat modeling, security design, secure development, security testing, and other cybersecurity assurance measures are built into the entire IDP process to minimize the introduction of vulnerabilities and deliver product versions with as few as possible vulnerability risks to customers.

Vulnerabilities are managed based on product/software version lifecycle milestones. Specifically, Huawei manages vulnerabilities in all product versions yet to reach the End of Service and Support (EOS) and releases vulnerability remediations (including mitigation measures, patches, and versions) for versions yet to reach the End of Full Service (EOFS) based on remediation policies in different lifecycle phases to help customers mitigate vulnerability risks on live networks.

Huawei Vulnerability Management Center identifies high-risk vulnerabilities that are of significant public concern and actively exploited, accelerates vulnerability response, and releases security notices (SNs) to affected customers within 24 hours. Once a vulnerability remediation is available, Huawei will release an SA to affected customers so that they can make informed decisions to mitigate risks.

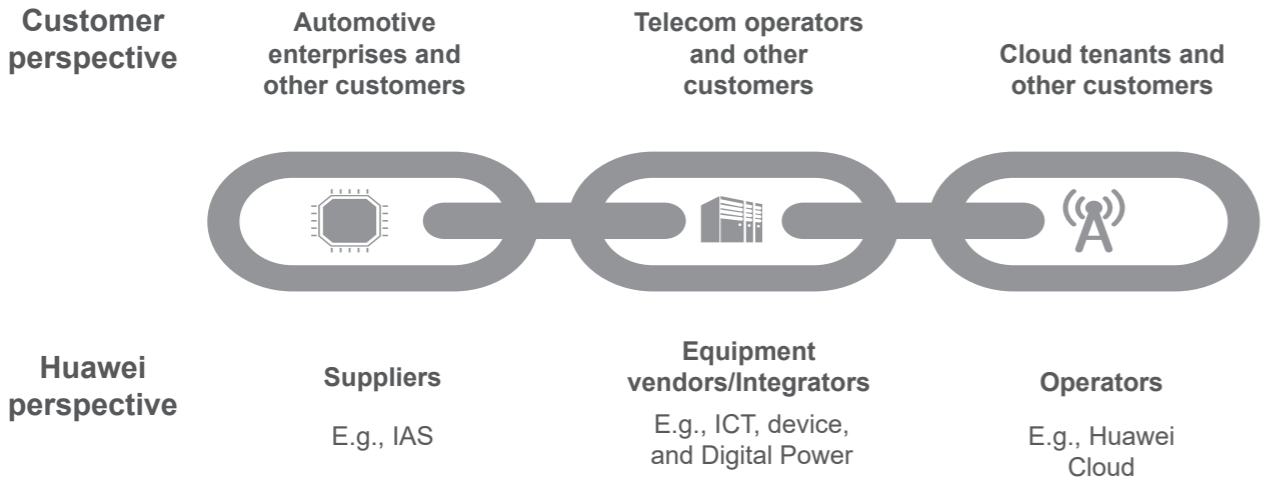
Figure 4-6 Vulnerability management throughout the product lifecycle



4.2.3 Supply Chain Management

Huawei has a wide range of product, service, and solution portfolios and serve different customers in the supply chain. It plays multiple roles, including as a supplier, equipment vendor/integrator, or operator. Playing such diverse roles has allowed Huawei to realize the importance of collaborative supply chain management from different perspectives.

Figure 4-7 Upstream and downstream roles in the supply chain

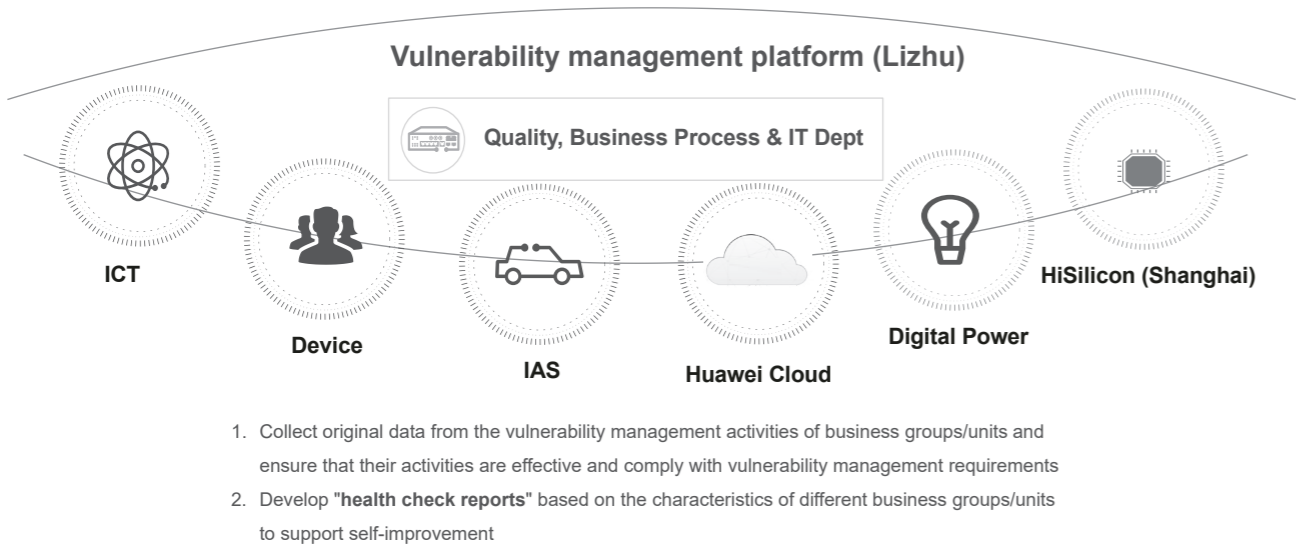


- As a supplier, Huawei has established a channel for prompt and accurate vulnerability awareness. Huawei has also developed a vulnerability disclosure website and a proactive communication channel for downstream equipment vendors/integrators, and continuously provides vulnerability remediations to support them in integrating and releasing remediations.
- As an equipment vendor/integrator, Huawei has established a vulnerability receiving, disclosure, collaboration, and response mechanism with suppliers. In addition, Huawei operates bug bounty programs to encourage security researchers and organizations to report suspected vulnerabilities in products. It has established a vulnerability disclosure website and a proactive communication channel to disclose vulnerabilities to customers in SAs, SNs, and release notes (RNs) and support customers in making informed decisions and mitigating vulnerability risks on live networks.
- As an operator, Huawei has established a vulnerability receiving, disclosure, collaboration, and response mechanism with equipment vendors and service providers. On the basis of live-network asset management, Huawei performs vulnerability awareness, assessment, remediation, and other activities to control live-network vulnerability risks at an acceptable level.

4.2.4 Vulnerability Management Platform

Huawei's ICT, device, IAS, and other business groups/units play different roles and hold different responsibilities. To ensure that business groups/units fulfill their responsibilities and support customers in vulnerability risk mitigation, Huawei has established a unified vulnerability management platform. This platform collects original data from the vulnerability management activities of business groups/units and generates a full picture of the vulnerability management levels and responsibility fulfillment status of business groups/units, enabling visualized and manageable vulnerability management results of all business groups/units. Huawei respects the differences among industries, drives continuous improvement of business groups/units, and provides customers with more efficient and professional vulnerability management support.

Figure 4-8 Vulnerability management platform



5 Summary

Huawei is fully aware of how important vulnerability management is to the security of the digital space. Consequently, it has developed an end-to-end system for full-view vulnerability management throughout the product lifecycle across the supply chain, in accordance with the five basic vulnerability management principles as well as industry standards and best practices. This is to support the mitigation of risks on customers' live networks.

As new technologies and threats continue to emerge and evolve, vulnerability management needs to be continuously iterated and optimized. Huawei is happy to share its experience and practices, build a collaborative and trusted ecosystem with customers and partners, and work together to address cybersecurity risks and challenges posed by vulnerabilities.

