KYOCERA Document Solutions Inc.

Kyocera Product Security

Version 072021/July 5, 2021

Table of Contents

Kyocera Commitment to Security of Products and Services

In recent years, cyberattacks have increased around the world. The various products connected to networks improve convenience while also exposing those products to the risks of the cyberattacks such as malicious unauthorized access and information leaks. To ensure that customers can use Kyocera products securely with ease, we commit to provide rigorous protection against these threats and minimize the risks with our security measures described in this document.

Security of Products and Services First

The security of products and services is always our top priority. Kyocera implements appropriate security measures in all phases of the product development life cycle. Especially given the "Security by Design" principle that security should be engineered into products at the earliest stage. Kyocera works hard not to create any vulnerabilities in the product from the outset. Also, after products are released to the markets, we continuously provide customers with secure products and services.

Product Development Life-Cycle Security

Kyocera takes strong security measures in product development lifecycle security, including planning, development, evaluation, production, and sales:

- In the planning phase, we continuously check for the newest security trends and vulnerability information. We learn from the vulnerability information to incorporate them into our new models and solve any security issues at an early stage.

- In the development phase, we actively utilize security design, secure programming, or static analysis tools for development. We also strictly check throughout the development process for potential vulnerabilities to ensure we do not embed any known issues.

- In the evaluation phase, we conduct testing not only within Kyocera but also conduct another security evaluation using an objective, independent third-party organization before releasing our products.

- In the production phase, we establish a secure environment and ensure secure production by strictly following procedures that enable us to perform precise operations.

Secure Operation

Even if sufficient security measures are taken at the time of product release, they may become insufficient later because new vulnerabilities are discovered daily. We continuously work hard to identify a security vulnerability, mitigate its impact, and take appropriate security measures against them after product release and operation.

Security Threats Analysis and Measures

Kyocera conducts threat analysis to proactively eliminate any vulnerabilities at the upstream stages of development. More specifically, we consider what assets need to be protected, what potential threats to the assets are, what the risks caused by the threats are, and what security measures should be taken against the risks. These are all incorporated in security requirements before development.

PSIRT

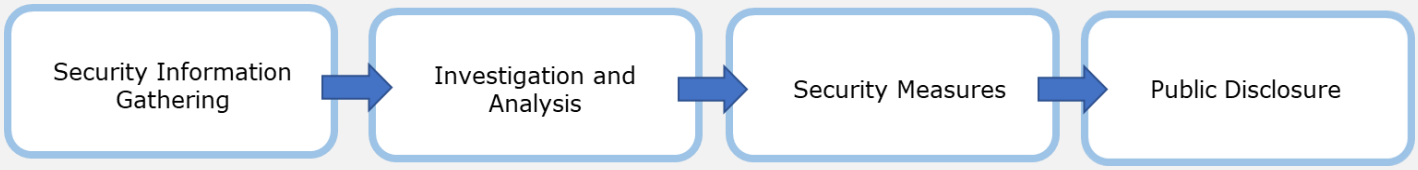
When an incident occurs, an organization must take immediate action. Kyocera has established a team called PSIRT (Product Security Incident Response Team) internally. PSIRT is composed of representatives from development, quality assurance, risk management, public relations, and Kyocera Group sales companies to quickly respond to security issues (i.e., vulnerabilities and incidents). PSIRT is an organization focused on risk management related to security vulnerabilities that potentially threaten the confidentiality, integrity, or availability of Kyocera’s products and services.

PSIRT has roles such as early detection of critical vulnerabilities in our products, prompt response to vulnerabilities in our products, and communication management with stakeholders.

When a vulnerability is found in practical, PSIRT takes appropriate action in accordance with the following incident handling process.

Incident Handling Process

Once a vulnerability is discovered, Kyocera focuses on responding promptly and appropriately, including responding to customers based on security vulnerability information. PSIRT generally proceeds in the following four steps: (1) gathering and sharing security vulnerability information, (2) investigating security issues and analyzing their impact on our products, (3) taking security measures against vulnerabilities, and (4) announcing to the public.



(1) Gathering and sharing security vulnerability information

We mainly check security information at an official open databases of vulnerability information such as CVE, JPCERT, and US-CERT, and search and obtain security information from the press such as newspapers and the Internet. More information is also provided by contacting the customer's nearest sales company or by inter-office members.

CVE: Common Vulnerabilities and Exposures
JPCERT: Japan Computer Emergency Response Team
US-CERT: United States Computer Emergency Readiness Team

(2) Investigating security issues and analyzing their impact on our products

At the development division, we investigate and analyze the phenomenon's effects when a vulnerability is exploited, the difficulty and conditions when a malicious attacker tries to exploit a vulnerability.

(3) Taking security measures against vulnerabilities

From above, if the results indicate that there is an impact, the development division continues to prepare technical and operational measures such as applying security patches.

(4) Announcing to the public

We make an announcement of our security measures via the Kyocera website, the PSIRT contact window, sales companies, or a service person.

The document is provided for information purpose only. The content of this document is subject to change from time to time without notice. Customers are responsible for making their own independent assessment of the information in this document and any use of Kyocera's products or services. The information in this document is provided "as-is" without warranty of any kind, whether express or implied. Although care has been taken when compiling this information, Kyocera makes no representations or warranties about the accuracy, completeness or adequacy of the information provided herein, nor fitness for a particular purpose, and shall not be liable for any errors or omissions. The only warranties for Kyocera's products and services are as set forth in the express warranty statements accompanying them. Nothing herein shall be construed as constituting an additional warranty.

KYOCERA Document Solutions Inc.

1-2-28 Tamatsukuri, Chui-ku, Osaka 540-8585, Japan
Phone: +81-6-6764-3555