

Vulnerability Management:

Version 1.0

December 19, 2017

Introduction

This document indicates our efforts against potential vulnerabilities to Kyocera products as well as measures against vulnerabilities if they are actualized. With measures described in this document, customers are able to use Kyocera products more safely.

Product development life-cycle security

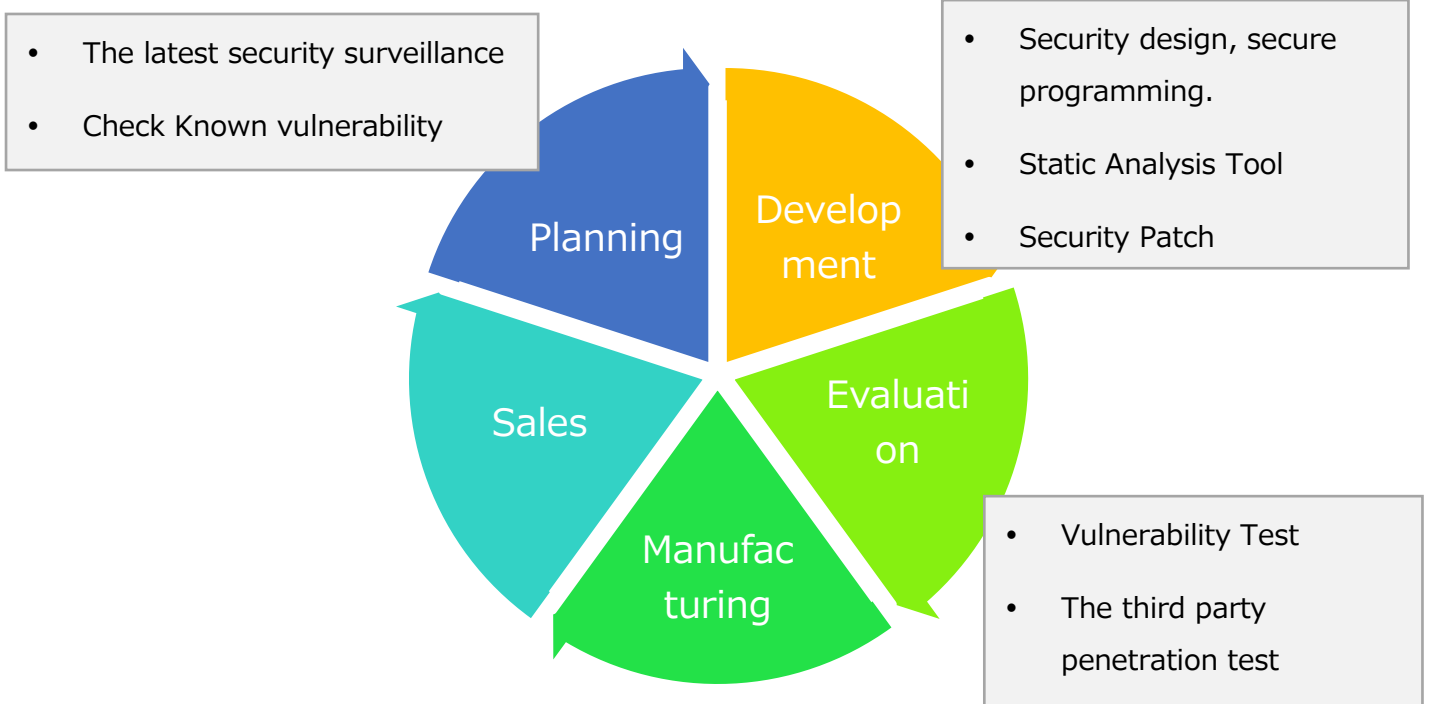
Kyocera has taken appropriate security measures in development life-cycle including planning, development, evaluation, manufacturing and sales.

In this series of development life-cycle from planning, development, and evaluation, we have taken measures to eliminate vulnerabilities.

In the phase of planning, we understand the current security trend and learn from information on vulnerability trying to solve any problems or issues in our newly developing machines at the earliest possible timing.

In the phase of development, we have actively utilized security design, secure programming or static analysis tool, etc. for development. Also, we have searched information on known vulnerability publicly available, and applied security patches, as appropriate, to get rid of vulnerability from our products severely checking throughout the development process.

In the phase of evaluation, we have conducted testing always suspecting if any vulnerability is lurked, or have another security evaluation conducted by the third-party organization from an objective perspective.



Computer Security Incident Response Team

For any potential vulnerabilities found after product release, we have established a customer-safety-first special process to respond to issues. We have established a team called CSIRT (Computer Security Incident Response Team) internally. This ad-hoc team is composed of representatives from organizations with each responsibility or role. This team acts promptly on investigation of the vulnerability-related issues, impact analysis, or handling issues. We handle any vulnerability found in cooperation with experts in all-related organizations in order to prevent our valued customers from any loss or inconvenience.

CRIST works on efforts according to the following phases.

- Gather information on vulnerability.
- Investigate issues and effect or impact of them on our products.
- Make an announcement to the public.

Kyocera promotes efforts against vulnerability based on above mentioned activities.



This document is provided for informational purposes only. The content of this document are 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, Chuo-ku, Osaka 540-8585, Japan

Phone: +81-6-6764-3555

<http://www.kyoceradocumentsolutions.com>

The information contained in this document is accurate and current as of December 2017 and is subject to update without prior notices.