Among the security enhancement initiatives that Fujitsu’s software product development divisions engage in are responding to vulnerabilities in open source software and human resources development, which we describe here.

**Software Security Quality Enhancement Initiatives**

To improve the security quality of its software products including firmware, Fujitsu conducts the activities shown in the diagram below, led by the Secure Software Development Promotion Team. Specifically, Fujitsu incorporates the following four activities into its development process to ensure security quality:

1. In the design process, Fujitsu conducts security analysis (threat analysis) and uses the results to improve the design.
2. In the implementation process, Fujitsu conducts coding to avoid any built-in vulnerabilities (secure coding), verifies source code using verification tools, and adds digital signatures to programs as necessary.
3. In the testing process, Fujitsu conducts security verification using verification tools and runs tests from a security perspective.
4. In the maintenance process, Fujitsu monitors security vulnerabilities, rapidly provides security patches, and publicly discloses security information in coordination with the Information-technology Promotion Agency (IPA) and the Japan Computer Emergency Response Team Coordination Center (JPCERT/CC).

For each process, Fujitsu deploys security architects with technical knowledge of security in each division, in order to entrench proper security responses in development activities. About 10% of all developers are certified as security architects.

**Overview of the Open Source Software Vulnerability Response System**

1. Fujitsu employs the Vulnerability Countermeasure Information Database JVN iPedia as an information source about open source software vulnerabilities. This database covers vulnerabilities which have been given a number by the National Vulnerability Database (NVD).
2. Based on information stored in the product repository, applicable open source software for each product is specified in the system for vulnerability information. This enables all open source software being used in products to be investigated for vulnerabilities.
3. Vulnerability information collected by the Open Source Software Vulnerability Response System is cross-checked against open source software divided by product in the product repository and immediately communicated to developers, starting the vulnerability response process.
4. Security is positioned as a high-priority issue and open source software vulnerabilities are given a high priority and investigated. Those responsible for product quality control in the product development divisions check the response status and issue appropriate instructions if they find the response to be lagging.

Various types of information publicly available on the Internet are used as source material.

*1 Vulnerability Countermeasure Information Database JVN iPedia is a vulnerability database jointly managed by JPCERT/CC and the IPA. It covers all vulnerability information registered in the NVD since 2007.
*2 The National Vulnerability Database is a vulnerability database managed by the U.S. National Institute of Standards and Technology.

**Product Developer Training**

Security training in software product development divisions follows two routes: Security Architect Training for professional human resources and General Training for general product developers and inspectors.

**Security Architect Certification System**

Security architects are those who have obtained professional qualifications within the Company to promote security response activities, enhance security quality in software products, and operate the Security Architect Certification System, which includes training programs given in software product development divisions.

The training program for security architects has a curriculum executed in four phases over several months for candidates recommended by each development division. The four phases are: (1) Prior learning and subjects, (2) Group training (exercise style), (3) Producing threat analysis reports, and (4) Certification review.

Following certification as a security architect, training programs are held regularly with details such as those listed below, at a rate of once or twice a year, to hone architects’ skills.

**Overview of the Open Source Software Vulnerability Response System**

1. **Product Repository**
2. **Open Source System Information Uptake**
3. **Vulnerability Notification**
4. **Response Result Reply**
5. **Situation Monitoring**

**Product Developer Training Map**

**Security Architect Training**

- Prior learning and subjects
- Group Training
- Writing and Submitting Reports
- Certification Review
- Security Analysis Methods
- Security Technology
- Vulnerability Expertise
- Secure Software Development Process
- Security Architect Certification

**General Training**

- New Employee Training
- Vulnerability Commentary
- Security Architects Instructing from Within Organizations
- Security Seminars with Outside Teachers
- e-learning Security for Beginners
- e-learning The Basic Security Development Process
- Group Training Security Application (Threat analysis exercises)
- Secure Development Process (Latest information)

**General Training and Education Program Subject List**

- Basic Security Knowledge
- Vulnerability Expertise
- Internal Incident Case Studies
- Security Application Knowledge
- Secure Development Process (Latest information)

**Skill Advancement Training Program Subject List**

- Describing Other Divisions’ Security Activities
- Internal Incident Case Studies
- Research Reports by Expert Organizations
- Secure Development Process (Latest information)