JPCERT-PR-2017-04
Issued: 2017-10-12

JPCERT/CC Activities Overview [July 1, 2017 – September 30, 2017]

Activity Overview Topics

- Topic 1 - Letter of thanks presented to persons who made significant contributions to cyber security activities

With the aim of minimizing damage caused by cyber security incidents taking place in Japan (herein, "incidents"), JPCERT/CC undertakes support activities to help respond to incidents, early warning activities to help prevent incidents, malware analysis, coordination activities related to vulnerabilities in software products, and other relevant activities. To ensure these activities are conducted smoothly and effectively, information and other forms of assistance are essential.

At JPCERT/CC, we have established a system for presenting letters of thanks as a sign of our deep appreciation to those individuals who have made particularly significant contributions with respect to cyber security activities. This year, we presented a letter of thanks and a commemorative shield to two recipients in July. One of the recipients was Shumpei Shimamura of clwit, Inc., who for many years has provided JPCERT/CC with analysis results of scan and attack activities targeting vulnerabilities. The information he provided was instrumental in analyzing Mirai malware, which triggered massive DDoS attacks in 2016, and in containing the damage in Japan. The other recipient was Recruit-CSIRT, which has provided JPCERT/CC with detailed information about APT attacks identified by Recruit Holdings Co., Ltd., and detailed analysis reports of vulnerabilities that presented a high degree of threat. The information provided by Recruit-CSIRT proved invaluable in efforts to prevent the spread of damage in Japan.

Letter of thanks presented to persons who made significant contributions to cyber security activities (Japanese)
https://www.jpcert.or.jp/press/priz/2017/PR20170725-priz.html

- Topic 2 - Response to ongoing reports of vulnerabilities in web application frameworks

Today, many web servers provide a variety of contents and functions using web applications. Web applications are often developed using a framework. Some of the more widely used frameworks include Apache Struts and Apache Tomcat, which are provided as open source software. Serious vulnerabilities have often been reported with these software applications, and the vulnerability in Apache Struts2

reported in March was subsequently exploited extensively, with many organizations both inside and outside Japan announcing damage including stolen information over the next six months.

When a vulnerability in open source software is reported, detailed information including attack codes may spread, promoting attack activities. Moreover, it often takes more time than expected to fix a vulnerability in a web server built using a web application framework, since it requires efforts on the part of the web server administrator as well as the web application developer. For this reason, when a new vulnerability is announced, accurate technical information must be communicated quickly so that both the web server administrator and web application developer can respond appropriately.

During this quarter, JPCERT/CC issued one CyberNewsFlash and three alerts regarding software vulnerabilities related to websites. With the vulnerabilities reported during this quarter in particular, we ensured that web server administrators were provided with the latest technical information so that they could respond without confusion. This was important because the PoC code was published shortly after announcement by the developer, new problems were soon identified with the released fixes, and the information released was updated several times. The information we provided included not only the information released by the developer but also the results of PoC code verification performed by JPCERT/CC and relevant information we collected on our own, as well as other technical information that served as a reference for the administrators and developers working on countermeasures.