JPCERT CC®

Japan Computer Emergency
Response Team Coordination
Center

JPCERT-PR-2014-04
Issued: 2014-10-09

JPCERT/CC Activities Overview [July 1, 2014 – September 30, 2014]

―Topic 1―　Awareness-raising campaign to mitigate the risk of password list-based attack

In an effort to address the situation with regard to losses and damage that continue to result from unauthorized logins due to password list-based attack, JPCERT/CC teamed up with Information-technology Promotion Agency (IPA) and conducted a joint campaign to raise awareness in Internet service users on the risk of using the same password for different services. To mitigate the risk of password list-based attack, appropriate account management will be required on the part of service users, in addition to measures implemented by service providers. Accordingly, with the help of service providers that authenticate service users with IDs and passwords, the joint campaign was launched, calling for service users to refrain from reusing the same password. As of October 9, 2014, this campaign is supported by over 20 businesses.

In August 2014, IPA published a report titled "Fact-finding Survey on Online Personal Authentication Methods." According to this report, approximately a quarter (25.4%) of the users use the same password used on websites providing services that involve financial transactions (Internet banking, online shopping, etc.) on other websites. The most common reason given by these users is that they are afraid they might "forget the password (if they use more than one password)" (64.1%). Under such circumstances, JPCERT/CC tallied the number of companies that suffered losses or damage from password list-based attacks based on publicly available information. This survey has found that various companies have continued to report losses or damage due to such attacks from 2013 to the present. To use online services safely, users must be aware of the risk involved in reusing passwords and practice appropriate management at all times.

To protect online service users, related industries are making ongoing efforts to understand the actual situation with regard to attacks, implement measures based on that understanding, and alert users to potential threats. Likewise, JPCERT/CC is collaborating with service providers and related agencies to help prevent the spreading of losses and damage by making available information on appropriate ways to manage passwords and avoid reusing them, and measures including the use of functions that prevent or alert users to unauthorized logins.

STOP Reusing Passwords!! Raising Awareness to Help Prevent Unauthorized Logins Due to Password List-based Attacks
https://www.jpcert.or.jp/pr/2014/pr140004.html#1

Seeking Corporate Support for the STOP Reusing Passwords!! Campaign
https://www.jpcert.or.jp/pr/2014/pr140005.html

－Topic 2－ Announcing a new numbering system for CVE numbers that identify vulnerabilities

The Common Vulnerabilities and Exposures (CVE) system, maintained and used by the MITRE Corporation to identify vulnerabilities, has been expanded as of January 1 of this year to be able to accommodate over 10,000 vulnerabilities per year. Under the new system, when the number of vulnerabilities exceeds 4 digits, the number of digits will be incremented by 1. If organizations referencing CVE employ mechanical processing based on fixed-length CVE numbers, those organizations could experience malfunction of their system. Accordingly, on January 15, 2014, the MITRE Corporation posted a notification on their CVE website that they are now operating under a new numbering system. This announcement was followed on July 15 by a reminder notification of the change of the CVE numbering system. Then on September 17, 2014, a new press release was issued to make the new CVE system known to CVE users including CVE Numbering Authorities (CNAs), as well as end users referencing vulnerability information. In conjunction with this release, JPCERT/CC, a CNA, also made an announcement on the new numbering system.

Notification of a New Numbering System for CVE Numbers that Identify Vulnerabilities
https://www.jpcert.or.jp/pr/2014/pr140006.html

MITRE Corporation Press Release
Leading Software Vendors and Cybersecurity Organizations Among Early Adopters of MITRE's New Vulnerability Naming Format
https://www.mitre.org/news/press-releases/leading-software-vendors-and-cybersecurity-organizations-among-early-adopters-of

List of Organizations and Agencies Supporting the New CVE Numbering System
Declarations of CVE-ID Syntax Compliance (MITRE Corporation)
https://cve.mitre.org/cve/identifiers/compliant_organizations.html

－Topic 3－ Android Secure Coding Seminar held in Delhi and Bangalore, India

In collaboration with CERT-In (National CERT of India) and Data Security Council of India (DSCI), JPCERT/CC held an Android Secure Coding Seminar in the Indian capital Delhi on September 10, and in Bangalore, located in southern India and home to many IT companies, on September 12.
Providing know-how related to Android secure coding to local software developers in India, where many Japanese companies develop their software, is expected to not only help raise awareness about

security-related matters among local developers, etc., but also contribute to the enhancement of Japanese software security.

The seminar was held as a one-day course consisting of lectures on the vulnerabilities of Android apps and exercises to deepen the understanding gained through the lectures. Participants in the seminar included Android programmers, development managers, and security researchers working for local major software vendors, foreign-capital IT companies, and financial institutions. Questions asked by the participants demonstrated the depth of their knowledge as well as their heightened awareness of security-related issues.

Android Secure Coding
http://www.slideshare.net/jpcert_securecoding/all-for-attendee

－Topic 4－ Appreciation Letter 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, analysis of malware, coordination activities related to vulnerabilities in software products, and other relevant activities. To ensure these activities are promoted smoothly and effectively, information and various assistance provided by individuals are inevitable. Today's society is hugely dependent on information and communication systems; if incidents are not handled effectively, society could face dire problems, with repercussions spreading across the globe.

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. In June 2014, we presented an appreciation letter and a commemorative shield to Takahiro Kato (General Manager, Business Promotion Department, Web Business Division, ICT Business Division, Toppan Forms Co., Ltd.) and Michael MOLSNER (Director of Information Security Lab, K.K. Kaspersky Labs Japan).

Appreciation letter presented to persons who made significant contributions to cyber security activities
https://www.jpcert.or.jp/press/priz/2014/PR20140703-priz.html