

Reporting Status of Vulnerability-related Information for Software Products, etc.

- 1st Quarter of 2006 (January - March) -

Information-Technology Promotion Agency (IPA) and JPCERT Coordination Center (JPCERT/CC), a limited intermediate corporation, have initiated to handle vulnerability-related information from July, 2004 based on the announcement “Standard for Handling Vulnerability-related Information for Software Products, etc. (#235, Announcement of METI, 2004) by the Ministry of Economy, Trade and Industry (hereinafter refers to METI).

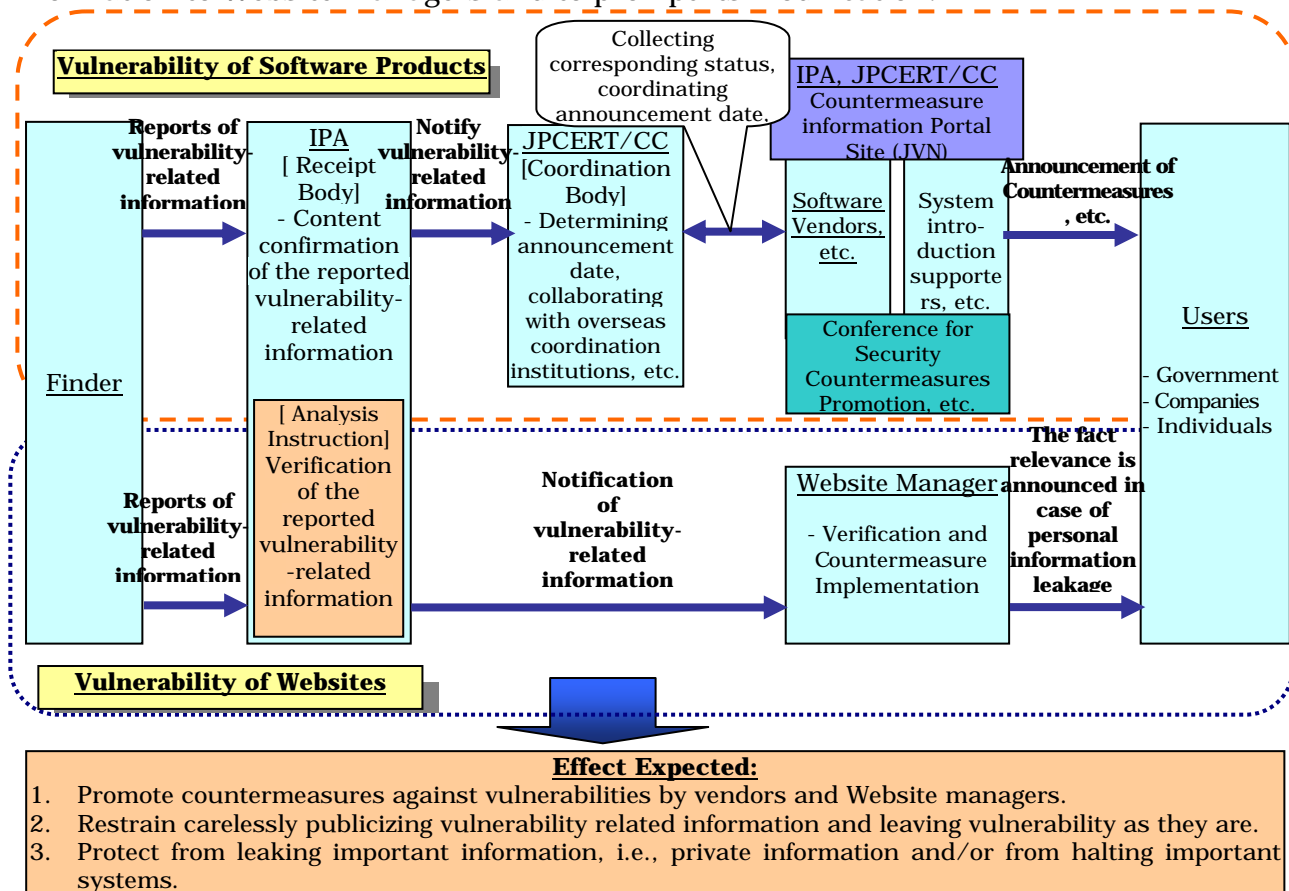
Based on the announcement, IPA is accepting reports for following vulnerability-related information:

1: Vulnerability-related Information for Software Products:

Vulnerabilities against software on clients such as on OSs and/or on browsers, software on servers such as Web servers, software embedded hardware such as IC cards, etc. Other than the information for vulnerability itself, information for verification method, attacking method and method for workaround are also accepted. IPA will notify such vulnerability-related information to JPCERT/CC and JPCERT/CC will communicate such information to concerned organizations such as vendors, etc. in domestic.

2: Vulnerability-related Information for Web Applications:

Vulnerabilities against systems which configure services unique to that site provided for public through the Internet Web sites, etc. IPA will notice such vulnerability-related information to Website managers and to prompt its modification.



“Information Security Early Warning Partnership” (Framework for Handling Vulnerability-related Information)

Source: Material for explanatory meeting for handling vulnerability-related information (General explanation for handling standard for vulnerability-related information in software and its guidelines) by the Ministry of Economy, Trade and Industry

Based on the framework for the vulnerability-related information described in advance, reporting status for the 1st Quarter of 2006 (January to March) is summarized as follows.

1. Reported Number:

The reported number in relation to vulnerability-related information reported to IPA from January 1 to March 31, 2006 was 106: of 34 was for vulnerability-related software products and the rest of 72 was for vulnerability-related Web applications. The cumulative reported number from the initiation of acceptance of reporting (July 8, 2004) was 674: of 167 was for vulnerability-related software products and the rest of 507 was for vulnerability-related Web applications. The Chart 1-1 shows the reporting status for respective quarters.

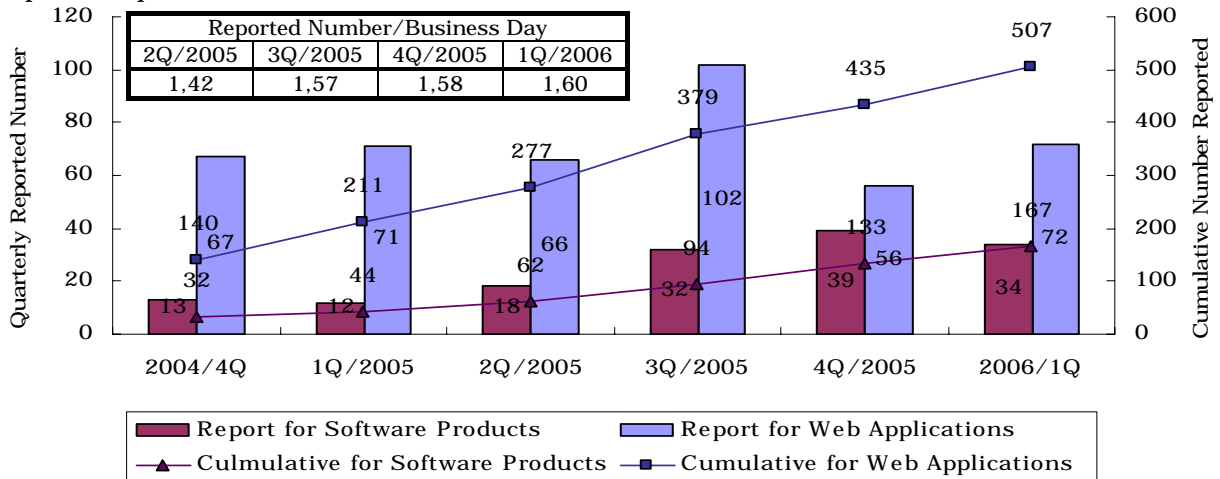


Chart 1-1: Quarterly Reported Number for Vulnerability-related Information

1) Handling Status of Reports

The Chart 1-2 shows the processing status of reports for the vulnerability-related information as of the end of March, 2006. As for software products, of 45% (61) of the reports being accepted as vulnerabilities (137) are modified and publicized. As for Web applications, of 56% (266) of the reports being accepted as vulnerabilities (472) are modified and publicized.

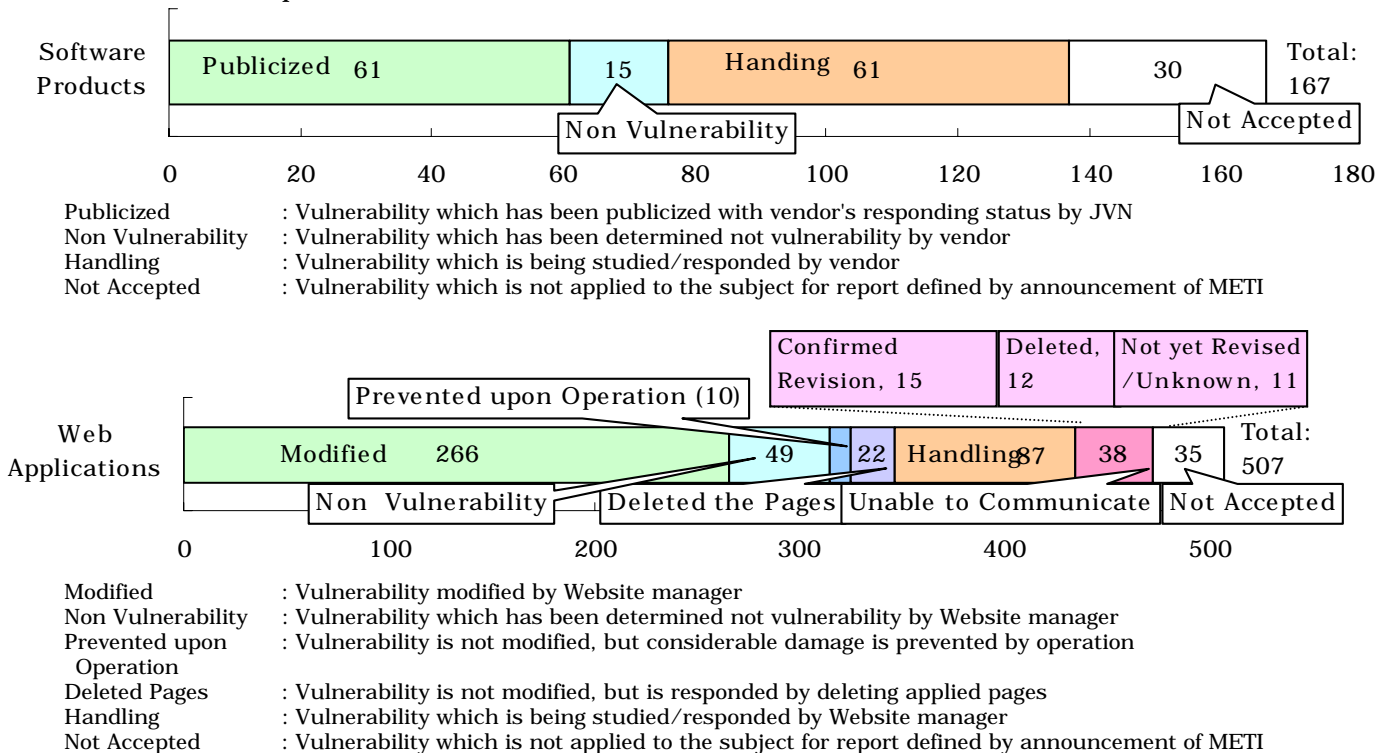


Chart 1-2: Processing Status of Reporting for Vulnerability-related Information (As of the End of March, 2006)

2. Handling of Vulnerability-related Information for Software Products and its Coordination:

The Chart 2-1 and 2-2 show the breakdown for the reports related to the vulnerabilities in software products reported to IPA for the dates from initial acceptance to the end of March, 2006. Reports related OSS (Open Source Software) were being increased from the 3rd Quarter of 2005. The most significant reporting was for Web browsers and the reporting for Web application software was subsequently followed.

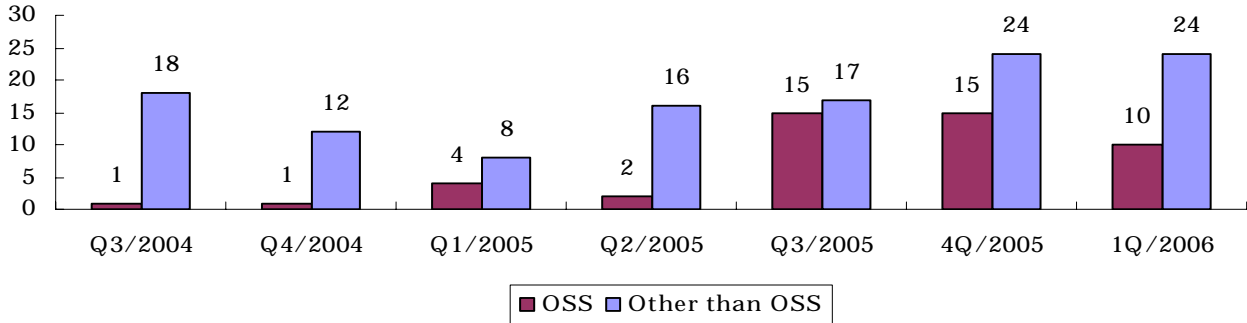
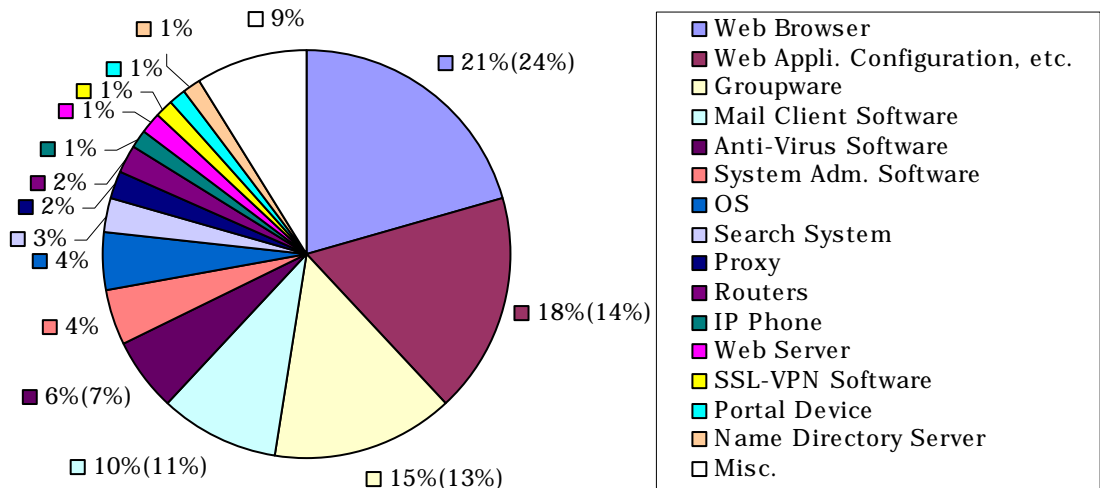


Chart 2-1: Breakdown of Vulnerabilities in Software Products (for the dates from Initial Acceptance to the End of March, 2006)



Home Appliances are included in the Misc. as they could be counted only 1 case each. (Breakdown of 137: Numbers in parenthesis are for previous Quarter)

Chart 2-2: Breakdown for Classification for the Vulnerabilities in Software Products (for the dates from initial acceptance to the end of March, 2006)

The Chart 2-3 shows the dates required for the announcement of vulnerabilities in software products. About 43% of reports were addressed within 45 days from its initial reporting and announced.

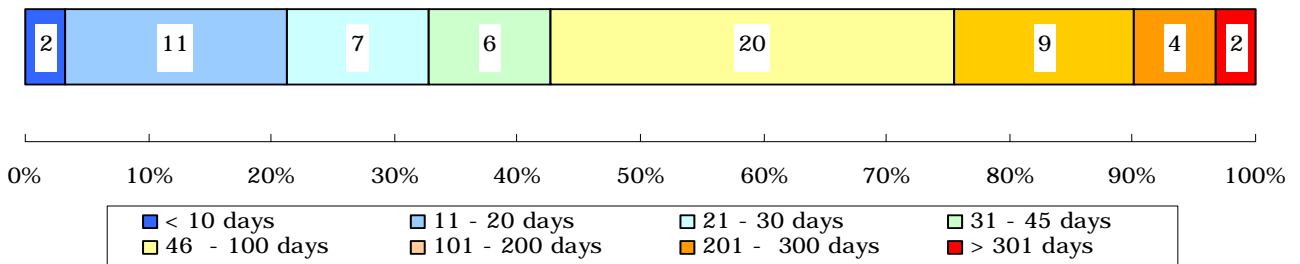
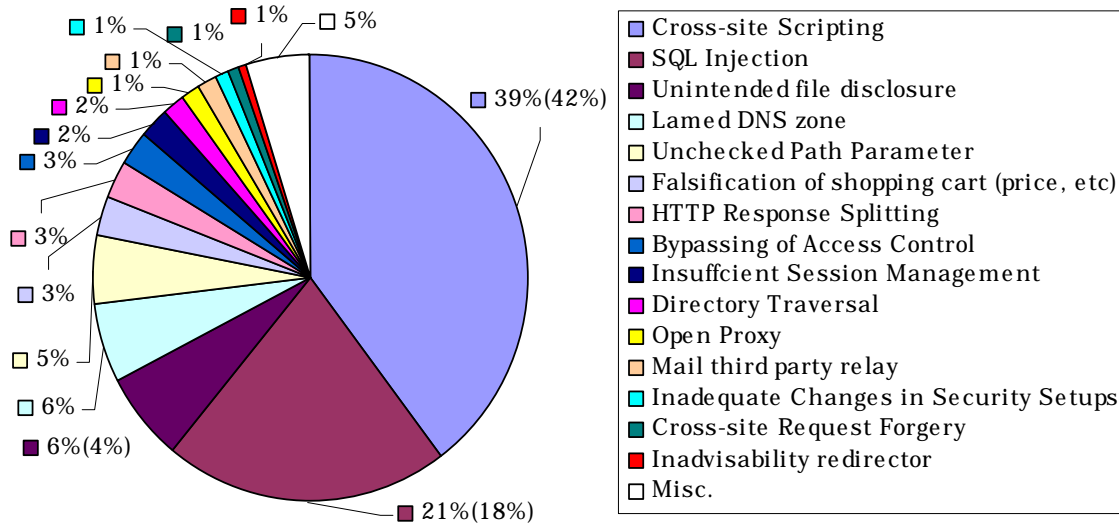


Chart 2-3: Dates Required for the Announcement of Vulnerabilities in Software Products

3. Handling of Vulnerability-related Information for Web Applications:

The total reports as information related vulnerabilities in Web applications reported to IPA were 507: of 472 information related vulnerabilities in Web applications being reported from its initial acceptance to the end of the 1st Quarter of 2006 excluding those not being accepted as they were not vulnerabilities is shown in the Chart 3-1.



- Breakdown of 472: Numbers in the parenthesis are for the previous Quarter

Chart 3-1: Breakdown of Vulnerabilities in Web Applications (for the dates from Initial Acceptance to the End of March, 2006)

In the type of vulnerabilities, the largest reporting was for "cross-site scripting" and "SQL Injection" subsequently follows. Most of all reports for "SQL Injection" were due to the detection of such pages which displaying error messages of database. Up to current, 64 cases had been addressed: of 38 cases was that "there was a problem about SQL Injection actually and was modified" so reported, the rest of 26 cases was that an error message had been displayed but could not insert SQL command actually: and are reported that there was not any problem about SQL Injection.

The increase in "Unintended File Disclosure" was by such reports that users' information could have been browsed by anybody because of insufficient setups of access control upon providing "shopping carts" on number of the Websites. Currently, the users' information is being inaccessible. The Chart 3-2 indicates the movement of the reported number for the "Unintended File Disclosure".

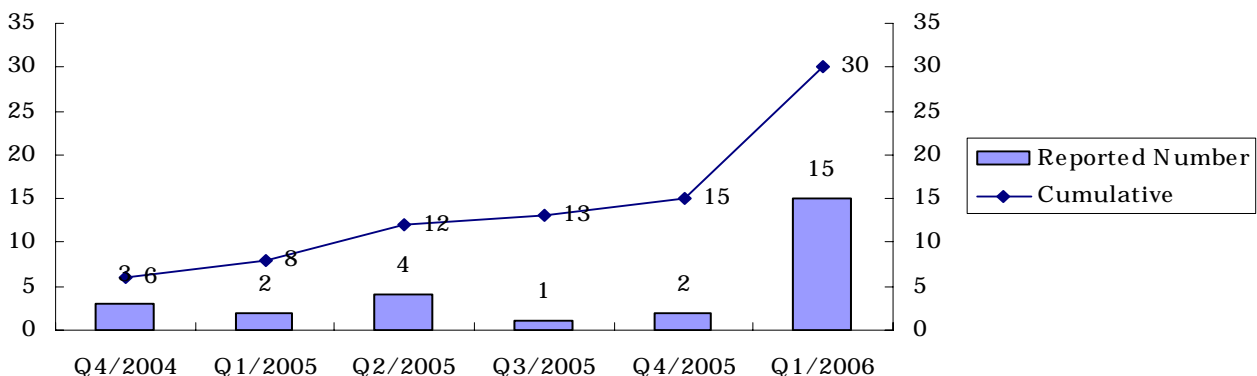


Chart 3-2: Movement of the Reported Number for the "Unintended File Disclosure"

The Chart 3-3 and 3-4 show dates required to modify vulnerabilities by type after notified detailed information of the vulnerabilities to Website managers. Of 81% of vulnerabilities reported against entire vulnerabilities reported were modified within 90 days.

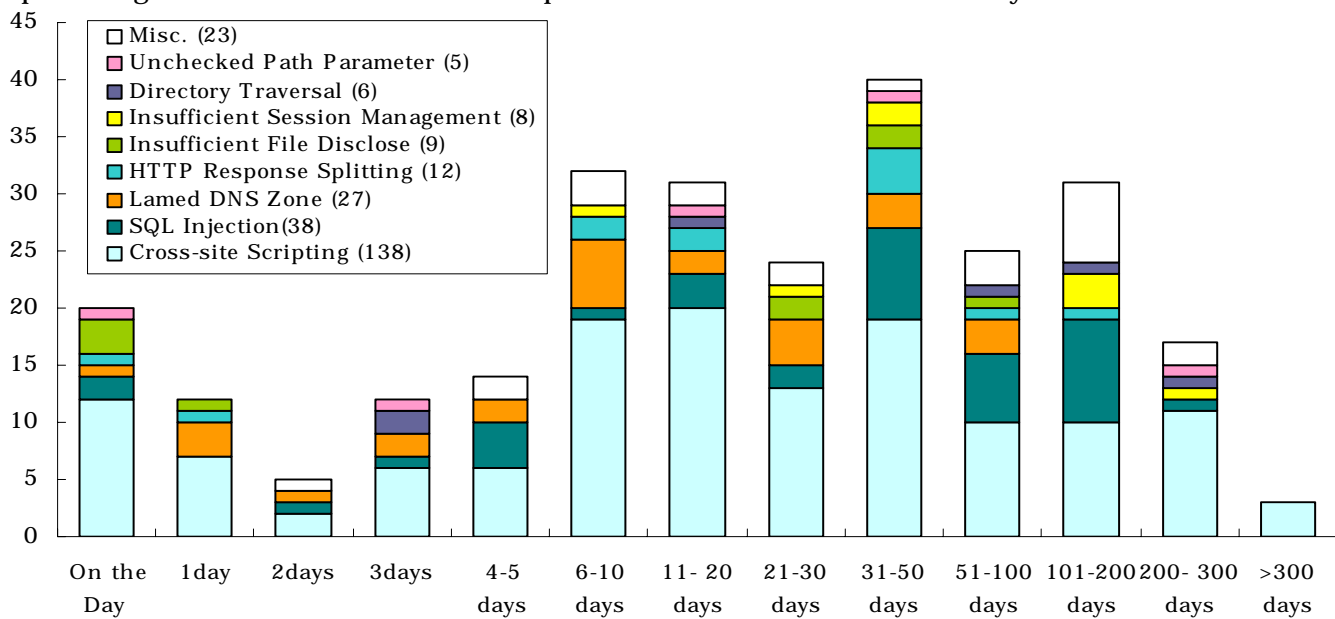


Chart 3-3: Dates Required Modifying Vulnerability in Web Applications

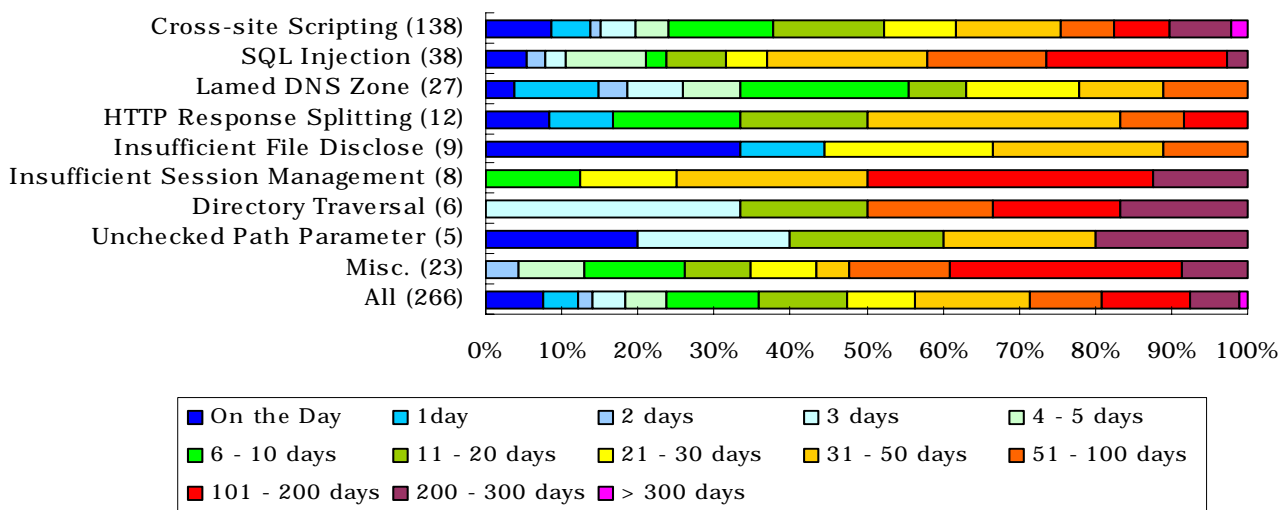


Chart 3-4: Dates Required Modifying Vulnerability in Web Applications by Type

Contact

IT Security Center, Information-technology Promotion Agency, Japan (IPA/ISEC)

Tel : +81-3-5978-7527

Fax : +81-3-5978-7518

E-mail : isec-info@ipa.go.jp