HIRT: Annual Report 2007

Hitachi Incident Response Team (HIRT)
http://www.hitachi.com/hirt/

Kashimada 890, Saiwai, Kawasaki, Kanagawa, 212-8567 Japan

1 Introduction

With the appearance of Internet worms in 1988, the importance of sharing information concerning the causes of incidents and countermeasures thereto was recognized, and the model of “incident response”, in which measures are taken in accordance with a pre-determined plan, began to take hold. From 2001 to 2003, network worms appeared and countermeasures against them spawned the model of “incident operations”. The incident operations represent a series of security moves implemented to predict and prevent damage caused by an incident and take measures to reduce the expansion of damage once such an incident has occurred.

In 2006, although there were fewer incidents such as network worms causing large-scale damage, there were increased cases in which the damage was not brought to public attention or where it was difficult to eliminate completely, such as targeted attacks at certain individuals or organizations, and information leakage, involving viral infections via P2P file exchange software.

To promote proactive measures against vulnerabilities, as well as reactive measures against incidents, as part of information security activities, such changes in the nature of incidents have meant an increasing need for Incident Response Teams (IRTs) to not only have the basic abilities to “predict and convey a threat from a technical point of view”, “perform technical adjustment activities” and “provide external communities with technical cooperation” but also provide the following function:

Implementing measures at an early stage in an effort to “catch any sign of future threats”

Hitachi Incident Response Teams (HIRT), as a organization with the above-mentioned abilities and roles, takes the lead in adopting proactive measures against vulnerabilities in products and services, as well as reactive measures against incidents, such as viral damage and information leakage, and assumes responsibility for establishing activities, mechanisms and systems to enhance the image of the Hitachi brand in the security field, as a unified point of contact for IRT activities in the Hitachi group.

This document gives you an overview of the threats and vulnerabilities in 2007, as well as HIRT activities, as the HIRT activity report for 2007.

2 Overview of activities in 2007

This section focuses on HIRT activities in 2007.

2.1 Overview of threats and vulnerabilities

In 2007, attack methods came increasingly diversified and sophisticated, such as the appearance of spam mail [1] using attached files, such as PDFs and MP3s, and the emergence of malware using websites as distribution media. Furthermore, as shown by the Storm Worm and Mpack, typical malware that uses websites as distributing media increasingly involve tricks that exploit the psychological weaknesses of users.

- Storm Worm

Storm worms started to spread in and around Europe on January 19, 2007 when a storm hit Europe. Disguising itself as the latest news on the storm, the original Storm Worm was distributed widely through the Internet via e-mail that urged users to execute an attached executable file. Subsequently, other types of storm worms appeared, with a URL contained in e-mail that redirected users to a malicious website, instead of having an executable attached to a single e-mail. These storm worms featured the use of news and events capable of attracting people’s attention.

- Mpack

Damage caused by Mpack was mainly reported in Europe in June 2007. Mpack is a malware program that modifies a normal webpage by inserting a tag containing a malicious website URL that induces users to download malware. When a user accesses the normal website, the inserted tag induces him/her to access the malicious website and download the malware unawares, resulting in his/her PC being infected [2].

Furthermore, a website is also used as a download site from which the invaded malware program downloads programs that repeatedly provide other functions. As you see, it can be said that the base for malicious activities is being shifted to websites.

As shown in Figure 1, the total number of vulnerabilities entered in the National Vulnerability

Database (NIST NVD) in 2007 is 6,690. (CERT/CC reported 7,236). Vulnerabilities in web application software products, including Cross-site Scripting (XSS), SQL Injection, Directory Traversal and Cross Site Request Forgery (CSRF), account for approximately 10% of the total, or 685. (See Figure 2.) [3]

Of the vulnerabilities in running websites reported to IPA, Cross-site Scripting (XSS) and SQL Injection account for approximately 70%, with the number of vulnerabilities reported increasing every year. (See Figure 3.)[4]

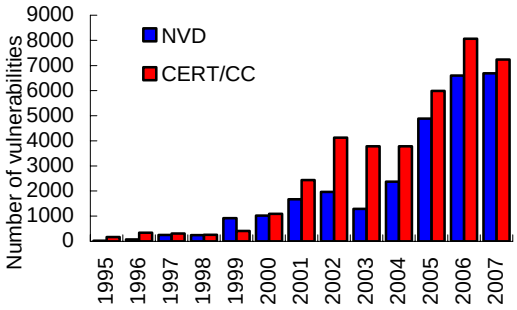


Figure 1: Changes in the number of vulnerabilities reported (Source: NIST NVD)

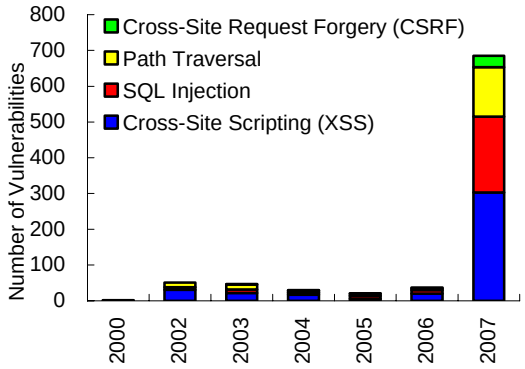


Figure 2: Changes in the number of vulnerabilities reported for web application software products (Source: NIST NVD)

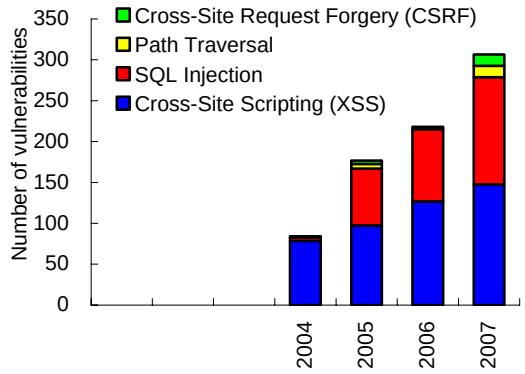


Figure 3: Changes in the number of vulnerabilities reported for websites (Source: IPA and JPCERT/CC)

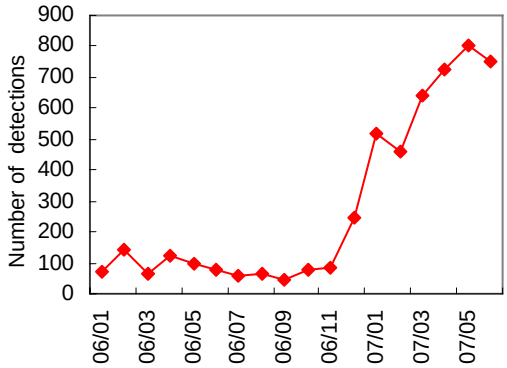


Figure 4: Changes in the number of SQL injection attacks detected (Source: LAC)

Reportedly, SQL Injection attacks detected have been increasing in number from 2007 onwards, as shown in Figure 4[5]. With this in mind, proactive measures against vulnerabilities need to be further promoted lest websites should provide a base for malicious activities.

Overall, it is now necessary to not only use a defensive mechanism to avoid bringing any malicious data, such as spam mail and malware programs, into an information system but also to combine it with a defensive mechanism to avoid the transfer of important data out of the information system by eliminating innate and potential threats.

2.2 HIRT activities

This subsection describes the HIRT activities in 2007.

(1) Starting HIRT open meeting that focuses on hands-on security training

A HIRT open meeting is an activity to let people know the HIRT community built on a trusting relationship. The meeting is held in accordance with the policy of "providing members of the HIRT/CC with the opportunity to exchange their opinions on HIRT activities", "providing a venue for the share of information to let the Hitachi group know about the activities of the HIRT/CC and receive opinions from people outside the HIRT/CC, and "asking people to participate in the HIRT community built on a trusting relationship".

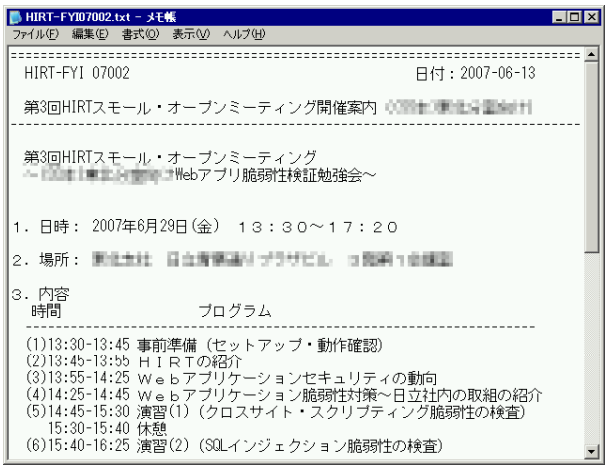
An HIRT open meeting for web application developers that focuses on hands-on security training was held twice in 2007, once in March and once in June, to give them more practical knowledge on implementing the "Web Application Security Guide". (See Figure 5)

(2) Static analysis methods and product security

There are two methods for examining a security flaw in a program: White box testing, where the source code is examined, and Black box testing, where various test cases are created in order to solve a problem by trial and error.

From 2006 onwards, Fazzing, a tool that allows users to input exceptional data using a tournament method to discover vulnerabilities in a program, started proliferating. This tool has successfully exposed much vulnerability to date. However, the tournament method does not always cover all vulnerabilities, hence the need to consider a static analysis method, which is less likely to overlook vulnerabilities and allows users to find vulnerabilities without using source code, as a means of examining a security flaw in products.

To cope with this situation, we invited Mr. Yuji Ukai from the Fourteen Forty Research Institute Inc. as an instructor in August 2007 to give us a lecture on how to use static analysis technology on the development side, including how it is used to inspect vulnerabilities in products.


HIRT-FYI07002.txt - メモ帳

ファイル(F) 編集(E) 書式(O) 表示(V) ヘルプ(H)

HIRT-FYI 07002 日付：2007-06-13

第3回HIRTスモール・オープンミーティング開催案内

第3回HIRTスモール・オープンミーティング
～Webアプリ脆弱性検証勉強会～

1．日時： 2007年6月29日(金) １３：３０～１７：２０

2．場所：

3．内容

時間	プログラム
(1)13:30-13:45	事前準備（セットアップ・動作確認）
(2)13:45-13:55	ＨＩＲＴの紹介
(3)13:55-14:25	Ｗｅｂアプリケーションセキュリティの動向
(4)14:25-14:45	Ｗｅｂアプリケーション脆弱性対策～日立社内の取組の紹介
(5)14:45-15:30	演習(1)（クロスサイト・スクリプティング脆弱性の検査）
15:30-15:40	休憩
(6)15:40-16:25	演習(2)（SQLインジェクション脆弱性の検査）

Figure 5: Notification of HIRT open meetings that focuses on hands-on security training

(3) Founding Nippon CSIRT Association

In April 2007, in order to establish a system that allows us to address problems that cannot be solved by IRT alone promptly and properly, and via a strong trusting relationship among IRTs, we founded the Nippon Computer Security Incident Response Team (CSIRT) Association with IIJ-SECT(IIJ), JPCERT/CC, JSOC(LAC), NTT-CERT(NTT) and SBCSIRT (SoftBank BB). [6] In addition, in order to share problems faced by each IRT, technical information and problem-solving methods at a higher level, each working group in the Nippon CSIRT Association has started activities to solve the problems.

(4) Applying for membership of WARP in the UK

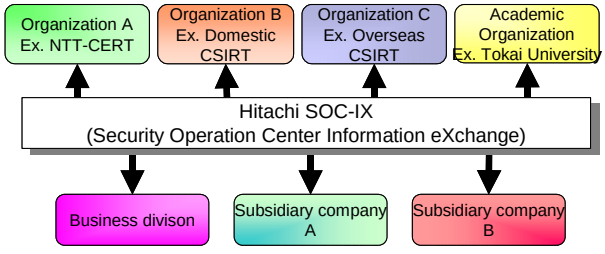
To strengthen the overseas partnership for IRT activities, we applied for membership of the Warning, Advice and Reporting Point (WARP) promoted by the Centre for the Protection of the National Infrastructure (CPNI), a security organization of the British government, and the application was granted on May 16, 2007.[7] WARP provides a framework for proactive measures against vulnerabilities, as well as reactive measures against incidents, promoted by a security organization of the British government, and is, at the same time, a community consisting of groups joining the framework.

(5) Strengthening the partnership with the IRT communities

As a part of activities to strengthen the partnership between organizations, we have held regular meetings with NTT-CERT[8] to exchange information to improve IRT activities since 2006. In 2007, we considered the joint use of observation data in order to establish a mutually cooperative relationship with NTT-CERT for observation of the Bot virus.

As for information leakage via file exchange software, we consider it necessary to establish a partnership with external organizations to assess the current situation and take appropriate measures. Obtaining assistance from the Association of Copyright for Computer Software that participates in the “Development of Technology to Detect Information Leakage through Networks and Automatically Stop the Circulation of Leaked Information”, a project run by the Ministry of Internal Affairs and Communications, we carried out an investigation of the network environment in which file exchange software is used. [9][10]

In future, we shall expand these partnership activities with other organizations to create the “Hitachi Security Operation Center Information eXchange (SOC-IX)”. SOC-IX is a framework in which organizations share and jointly use the required information to analyze threats and predict future ones, including observation data. (See Figure 6.)



Creating a framework or mechanism for exchange information, such as observation data, has the following advantages:
- It allows analysis using a large amount of various observation data.
- It allows you to use observation data you do not have
- It allows you to use technology and know-how in fields in which each CSIRT excels.

Figure 6: Schematic view of the Hitachi SOC-IX

(6) Publication of IRT activities

As we also consider conveying IRT activities to be necessary for promoting information security measures, we set up a website (http://www.hitachi.com/hirt/publications/) that provides an overview of our HIRT activities as a report in January 2007. We published six reports there (three in English) in 2007. (See Table 1.)

(7) Other activities

- Cooperated in creating test questions for "Network Test 2007" conducted by the Nikkei Network.
- Contributed an article on vulnerability measures to the Nikkei Business Publication's ITpro Computer Security Incident Response Team (CSIRT) Forum.
- Contributed an article on "How to Use Websites Providing Information on Vulnerability Measures" to a security portal site run by the National Police Agency (@police). [11]

Table 1: Reports published on our website

Number	Title
HIRT-PUB07012	Investigation report on information leakage caused by P2P file exchange software in 2007
HIRT-PUB07007	Overseas Security community - UK WARP
HIRT-PUB07004	Behavior of worm-infected packets
HIRT-PUB07003	Information Security Day
HIRT-PUB07002	Providing Hitachi security information via the RSS directory
HIRT-PUB07001	An animated movie of HIRT activities

3 HIRT

To give you an in-depth understanding of HIRT, this section describes the organizational model adopted, the HIRT/CC, a coordinating organization, and the activities currently promoted by the HIRT/CC.

3.1 Organizational model

We have adopted an organizational model consisting of four IRTs. (See Figure 7 and Table 2.) The four IRTs consist of three IRTs; each of which corresponds to an aspect of the Hitachi group and the HIRT Coordination Center (HIRT/CC), an IRT that provides coordination among the three. The first aspect is that which develops products related to information systems (Product Vendor IRT). The second is one that builds a system or provides a service using those products (SI Vendor IRT).

The third aspect is one that administers Hitachi's information systems as an Internet user (Internal User IRT). Such classifications not only clarify the role each IRT has to play but also promote security activities effectively and efficiently in partnership among the IRTs. Please also note that HIRT refers to incident operation activities within the entire Hitachi group in a broader sense, and the HIRT/CC in a narrower sense.

As shown in

Table 3, we experienced four phases before four IRTs had been established. After the roles and functions of the three IRTs had been roughly decided, the HIRT/CC was formed as a coordinator for the internal and external IRTs. In addition, each phase has a trigger that causes a corresponding IRT to be formed. For example, Multiple Vulnerabilities in Many Implementations of SNMP [12], as reported by CERT/CC, worked as a trigger to form the Product Vendor IRT in the second phase, while in the third, the start of an "Information Security Early Warning Partnership" worked as a trigger to establish the SI Vendor IRT.

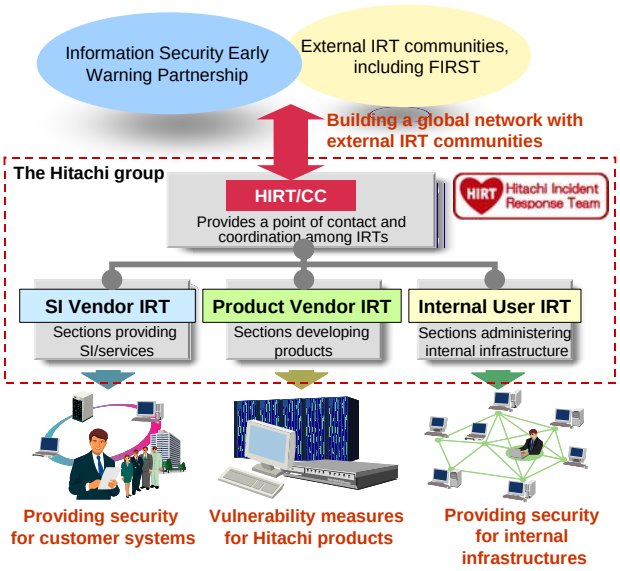


Figure 7: Four IRTs as an organizational model

Table 2: Role of each IRT

Category	Role
HIRT/CC	Corresponding sections: HIRT/CC - Provides a point of contact to external IRT organizations, such as FIRST, JPCERT/CC and CERT/CC. - Provides coordination among the SI Vendor, Product Vendor and Internal User IRTs.
SI Vendor IRT	Corresponding sections: Sections providing SI/services - Promotes IRT activities for customer systems. - Provides customer systems with equivalent security against reported vulnerabilities to that for internal systems.
Product Vendor IRT	Corresponding sections: Sections developing products - Provides support to promote vulnerability measures for Hitachi products and the release of information concerning such measures - Promptly investigates whether a reported vulnerability has an impact on Hitachi products, notifies users of the impact, if any, and provides a security fix.
Internal User IRT	Corresponding sections: Sections administering internal infrastructures - Provide support to promote security measures for internal networks lest Hitachi websites should be used as a base for making unauthorized access.

Table 3: Phases until the organization was formed

Phase	Overview
April 1998	We started IRT activities as a project to establish a Hitachi IRT framework.
1st phase Establishing the Internal User IRT (1998 - 2002)	In order to run a Hitachi IRT on a trial basis, we formed a cross-sectional virtual team within the Hitachi group to start mailing list based activities. Most of the members comprised internal security experts and those from sections administering internal infrastructures.
2nd phase Establishing the Product Vendor IRT (From 2002 -)	In order to start conducting activities seriously as a Hitachi IRT, the sections developing products played a central role in establishing an organizational structure of the Product Vendor IRT with related business sites through cooperation from internal security experts, the sections administering internal infrastructures, the sections developing products and the Quality Assurance Department.
3rd phase Establishing the SI Vendor IRT (From 2004 -)	We started to form an SI Vendor IRT with the sections providing SI/services. In order to implement proactive measures against vulnerabilities, as well as reactive measures against incidents, swiftly via partnership with Internet communities, we started to form HIRT/CC, which provides a point of contact for external organizations and enhances coordination among Internal IRTs.
October 2004	We established the HIRT/CC.

3.2 Positioning of the HIRT/CC

The HIRT/CC is an executive organization of the Product and Service Security Committee under the Information and Telecommunication Systems. Its main activities include promoting security activities in terms of technology and systems through mutual cooperation with the Information Security Administrative Department, Information System Business Division, and Quality Assurance Division, helping each business division and group company implement proactive measures against vulnerabilities, as well as reactive measures against incidents, and promoting security measures through partnerships among organizations as a point of contact for IRT activities in the Hitachi group (See Figure 8).

The organization of the HIRT/CC features the adoption of a model in which organizations on the vertical axis and communities on the horizontal axis collaborate with each other. More specifically, this model has achieved a flat and cross-sectional organization for implementing measures and provided a role for coordinating distributed functions by creating a virtual organization consisting of dedicated personnel and those who are assigned to HIRT activities as an additional task. Such organization is based on the concept that the performance of duties by each section and cooperation among sections are necessary to solve security issues, given the great diversification among components in the information systems.

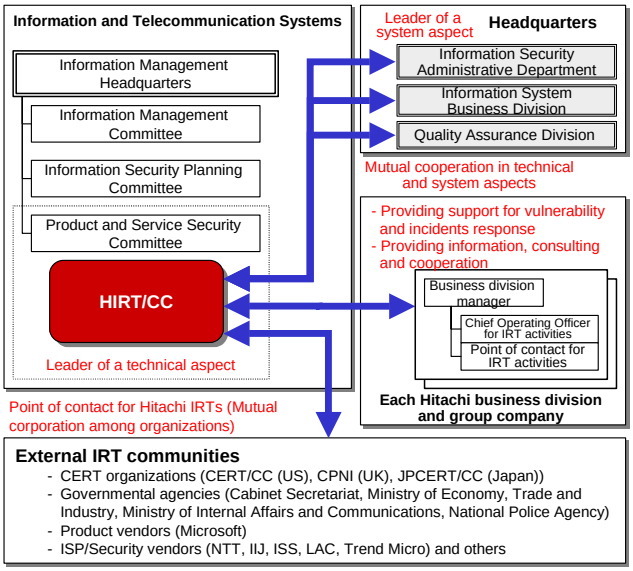


Figure 8: Positioning of the HIRT/CC

3.3 Main activities for the HIRT/CC

Table 4 shows the main activities currently promoted by the HIRT/CC. Regular activities include collaboration with domestic and overseas organizations in IRT activities and activities for internal and external organizations. The activities for internal organizations include providing sections/persons in charge of development processes with feedback on know-how obtained through the collection and analysis of security information in the form of guidelines or support tools, and providing internal organizations with such know-how by issuing a document or advisory calling attention to the same. The activities for external organizations include notifying Internet users of our security efforts for the products and services of the Hitachi group through our security portal website.

As for the issue of documents for calling attention and advisories, HIRT security information has been broken down into two types since June 2005: HIRT security information that needs to be distributed widely simply to attract attention and HIRT-FUP information used to ask a section or person to take reactive measures. We have adopted two types of information issue by taking its priority and the need for its release into account. (See Table 5 and Figure 9.) In order to convey information efficiently, aggregating the same reduces the number of issues of information, and the release of information is performed in collaboration with the Information Security Administrative Department and Quality Assurance Division.

Table 4: Promoted projects

Category	Overview
Collecting, analyzing and providing security information	- Issues a document calling attention and advisory. - The horizontal deployment of information and know-how concerning proactive measures against vulnerabilities, as well as reactive measures against incidents
Strengthening the domestic partnership for IRT activities	- Promotes collaboration activities among IRTs, including the provision of a point of contact on addressing an incident. - Holds regular meetings with domestic IRTs that are membership of FIRST (NTT-CERT, IIJ, JPCERT/CC, etc.).
Strengthening the overseas partnership for IRT activities	- Establishes a collaboration system with overseas business units in the Hitachi group. - Establishes a collaboration system with overseas product vendor IRTs (Using FIRST PST meetings). - Conforms to vulnerability-related standards, such as CVE and CVSS.
Taking proactive measures against product vulnerabilities, and promoting provision of information through a strengthened partnership with Hitachi group companies	- Adjusts proactive measures against vulnerabilities, as well as reactive measures against incidents, in the Hitachi group with internal and external organizations, when a vulnerability emerges in a Hitachi product or a Hitachi-related website. - Shares management processes for software products, built-in products, and services, and refines development processes - Provides guidelines for secure software/system development, expands and diversifies support tools, and makes them available to the Hitachi group. - Discloses information concerning proactive measures against vulnerabilities in Hitachi products to external organizations and promotes the circulation of information (using the our security portal website).
The thorough implementation of measures against vulnerabilities in website applications for external users	- Performs activities to enhance security awareness so that a security culture takes root. - Refines website development processes (guidelines for developing, inspecting and running websites)
The broadening presence of Hitachi in security	- Establishes a joint research system between Tokai university (Professor Kikuchi) and HIRT. - Adds more value to the Hitachi SOCIX (Security Operation Center Information eXchange) - Enriches the content of IRT activity websites for external users.

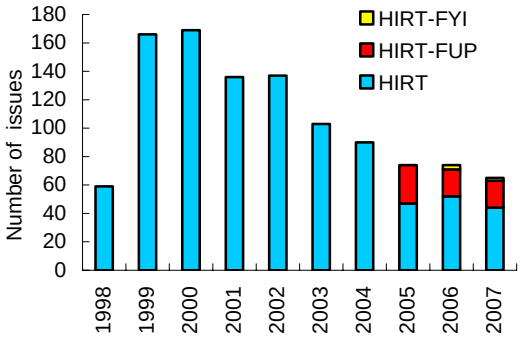


Figure 9: Number of issues of security information by ID number

Table 5: Classification of security information issued by HIRT

ID number	Usage
HIRT-FUPyynnn	Priority: Urgent Distributed to: Only related sections Is used to notify related sections of a vulnerability when an HIRT member has found such vulnerability in a Hitachi group product or a website, or received such information.
HIRT-yynnn	Priority: Middle - high Distributed to: No restriction Is used to widely call attention to proactive measures against vulnerabilities, as well as reactive measures against incidents.
HIRT-FYIyynnn	Priority: Low Distributed to: No restriction Is used to notify people of HIRT open meetings or lecture meetings.

4 Activity summary from 1998 to 2006

This section describes the activities for each year from 1998 when the HIRT project started.

4.1 Year 2006

(1) Providing a unified point of contact for vulnerability report notifications

In order to circulate vulnerability-related information properly in the Hitachi group and thereby promote measures against vulnerabilities in Hitachi software products and websites, we provided a unified point of contact for notifying vulnerabilities found in software products and web applications in November 2006.

(2) Enhancing Web application security

In October 2006, as part of web application security measures in the Hitachi group, we created guidelines and checklists and provided support for their implementation in the Hitachi group. We updated “Web Application Security Guide (Development) V2.0” by adding new

vulnerability items, such as LDAP and XML injection, and a method for checking the existence of such vulnerabilities.

(3) Calling attention to information leakage caused by P2P file exchange software

Antinny is a virus that appeared in August 2003 and is widespread through "Winny", file exchange software. The virus continues to cause information leakage from infected files and attack particular sites. In April 2006, HIRT created a leaflet entitled "Prevention of Information Leakage Caused by Winny and Proactive Measures against Winny" based on previous experience of threats, to call attention to it.

(4) Starting product security activities for digital home appliance and their embedded software

We have started product security activities for digital home appliance and their built-in software. HIRT focused on the Session Initiation Protocol (SIP), a call control protocol for Internet telephony, in order to summarize related security tools and measures into a report.

(5) Strengthening the partnership with IRT communities

In March 2006, we introduced Hitachi's IRT activities in a workshop held by NTT-CERT to exchange information to improve IRT activities.

(6) Improving security for external sites connected and promoting proactive measures against vulnerabilities

In November 2006, with a view to "improving security for external sites connected and promoting proactive measures against vulnerabilities", we held an HIRT open meeting for security managers and server administrators in business divisions. During the meeting, we described the vulnerabilities detected in monthly vulnerability reports and preventive measures for the same.

(7) Lecture meetings held in 2006

- May 2006: "Security for embedded systems", by Mr. Yuji Ukai, eEye Digital Security
- September 2006: "Measures against Botnets in Telecom-ISAC Japan", by Mr. Satoru Koyama, Telecom-ISAC Japan

(8) Other activities

- Gave a lecture in the Security Implementation Course for Web Application Developers provided by the Information-Technology Promotion Agency, Japan.[13]
- Started adding a digital signature to technical documents (PDF files) issued from HIRT.[14]
- Contributed articles to Microsoft Security Column and FIRST Conference.[15][16]

4.2 Year 2005

(1) Joining FIRST

In January 2005, in order to boost experience in IRT activities, create an organizational structure to address incidents that allows us to form a partnership with organizations in foreign countries, and collect more accurate information promptly, we joined the Forum of Incident Response and Security Teams (FIRST), an international community for computer incident handling teams.[17] The preparation period extended for about one year, since any team wishing to join the community must obtain recommendations from two member teams before doing so.

As of January 2008, the eleven Japanese teams that are community members include CFC (Info-Communications Bureau of the National Police Agency), HIRT (Hitachi), IIJ-SECT (IIJ), JPCERT/CC, JSOC(LAC), NCSIRT (NRI Secure Technologies), NISC (National Information Security Center), NTT-CERT(NTT), SBCSIRT (Softbank BB), RicohPSIRT (Ricoh) and YIRD (Yahoo). (See Figure 10.)

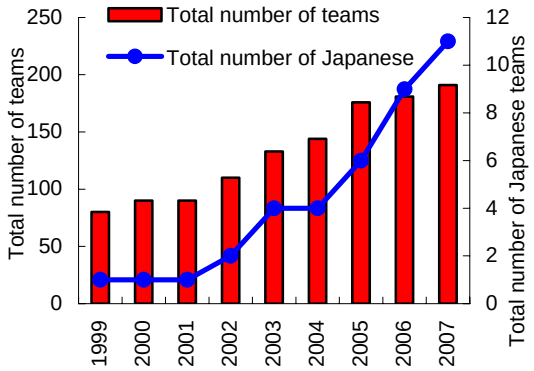


Figure 10: Changes in the number of members of FIRST

(2) Setting up a security information portal site

In September 2005, in order to provide Internet users with comprehensive information on security problems applicable to the products and service of the Hitachi group, we set up a security information portal site within which the security information provided through the websites of Hitachi business divisions and group companies is integrated. (See Figure 11.) We also created "Guidance for Providing Security Information from Websites to External Users, V1.0".

Security information portal site:
Japanese: http://www.hitachi.co.jp/hirt/
English: http://www.hitachi.com/hirt/

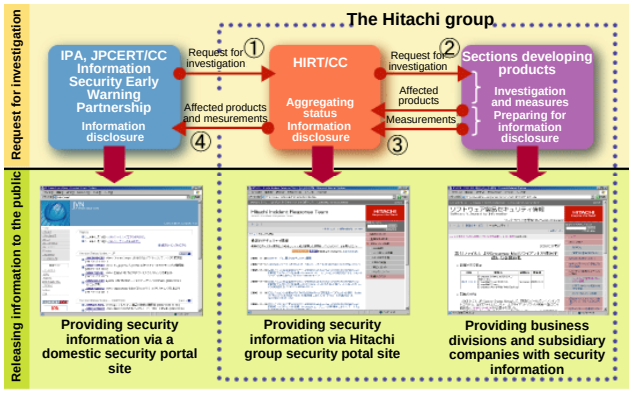


Figure 11: Providing security information from the security information portal site

(3) Strengthening the domestic partnership for IRT activities

In order to strengthen the domestic partnership for IRT activities, we hold meetings with domestic teams that are members of FIRST, and individual meetings with NTT-CERT and Microsoft Product Security Team (PST), and created an emergency call network to be used, for example, when a website is found to have been tampered.

4.3 Year 2004

(1) Participating in Early Alert Partnership System for Information Security

The Early Alert Partnership System for Information Security started in July 2004 when the "Standard for Handling Information Related to Vulnerabilities in Software, etc." was implemented.[18][19]

The Hitachi group registered Hitachi as a development vendor to the partnership system, using HIRT as a point of contact, and started publishing how measures against vulnerabilities in products could be implemented in JP Vendor Status Notes (JVN).[20]

(2) Enhancing web application security

In November 2004, we created the "Web Application Security Guide (Development), V1.0" and distributed it throughout the Hitachi group. The guide summarizes typical problems that need to be considered when designing and developing web applications, and provides an overview of measures taken to solve such problems.

(3) Lectures given in 2004

- January 2004: "Security business affairs after Blaster in the US", by Mr. Tom Noonan, President and CEO of Internet Security Systems (ISS)

4.4 Year 2003

(1) Starting web application security activities

We started to consider a method for enhancing web application security and developed the "Procedure for Creating a Security Measure Standard for Web Application Development V1.0" with business divisions.

(2) Disseminating vulnerability information from NISCC throughout Hitachi

Following the dissemination of vulnerability information from CERT/CC in 2002, we started obtaining information from NISCC (currently, CPNI) based on the Vulnerability Disclosure Policy. It was 006489/H323 of January 2004 when information on a Hitachi product was first published in NISCC Vulnerability Advisory after starting the activity.[21]

(3) Providing a point of contact for organizations external to HIRT

In line with the more active reporting and releasing of information concerning the discovery of a vulnerability ([22], [23], and [24]), we provided a point of contact, as shown in Table 6, that initiates actions when vulnerabilities or malicious actions in Hitachi products and Hitachi-related websites are pointed out.

Table 6: Information on point of contact

Name	"HIRT": Hitachi Incident Response Team.
Address	890 Kashimada, Saiwai, Kawasaki City, Kanagawa Prefecture, 212-8567
E-mail	hirt@hitachi.co.jp
PGP key	KeyID = 2301A5FA Key fingerprint 7BE3 ECBF 173E 3106 F55A 011D F6CD EB6B 2301 A5FA pub 1024D/ 2003-09-17 HIRT: Hitachi Incident Response Team < hirt@hitachi.co.jp >

4.5 Year 2002

(1) Disseminating vulnerability information from CERT/CC throughout Hitachi

SNMP vulnerability [12] reported from CERT/CC in 2002 affected a wide range of software and devices. This provided an opportunity to start the Product Vendor IRT and obtaining information from CERT/CC based on the Vulnerability Disclosure Policy.[25] It was VU#459371 of October 2002 when Hitachi product information was first published in the CERT/CC Vulnerability Notes Database after commencing this activity .[26]

(2) Assisting JPCERT/CC in building Vendor Status Notes

JPCERT/CC Vendor Status Notes (JVN) were released to the public for the first time in February 2003 in the form of a trial website (http://jvn.doi.ics.keio.ac.jp/). (See Figure 12.) [27][28] With the implementation of the "Standard for Handling Information Related to Vulnerabilities in Software, etc." in July 2004, the roles

of the trial site were transferred to a site releasing information on reported vulnerabilities (http://jvn.jp/).

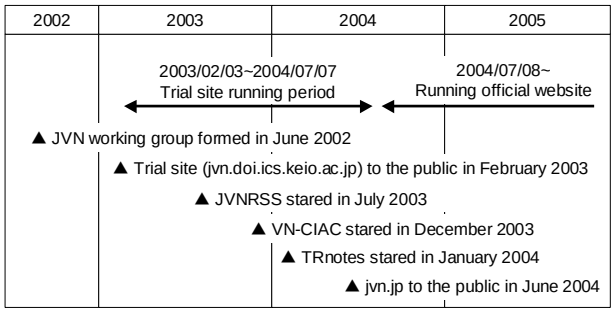


Figure 12: Building and running a JVN trial site

4.6 Year 2001

(1) Investigating the activities of worms attacking web services

We investigated the activities of worms attacking web services in 2001, CodeRed I, CodeRed II and Nimda, from June 15, 2001 to June 30, 2002, based on the log data from the websites on the Internet. For CodeRed II and Nimda (Figure 13), which caused significant damage in Japan, the log reveals that the time span between the time at which the attack was first logged and the date on which attacks occurred most frequently was only approximately two days, indicating that damage caused by the worms had spread rapidly and widely.

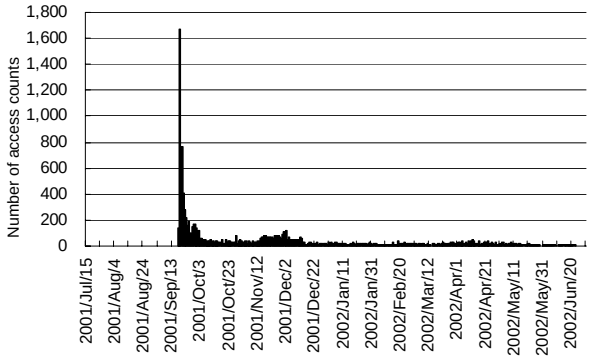


Figure 13: Changes in the number of access counts found during the observation period (for Nimda)

4.7 Year 2000

(1) Investigating the severity metrics for vulnerabilities

In order to measure the vulnerability severity level used for destructive or security-compromising activities, we investigated the severity metrics used by related organizations in order to summarize the results into a report.

CERT/CC publishes notes called “Vulnerability Notes” [29] for vulnerability. The “Vulnerability Notes” contain the several metrics, one of which is Severity Metric indicating the severity of vulnerability. [30] Common Vulnerabilities and Exposures (CVE) classifies information security vulnerabilities into “Vulnerabilities” and “Exposures” and focuses on only the former [31]. The former is defined as mistakes in software that can be directly used by a hacker to gain access to a system or network. The latter is defined as system configuration issues or mistakes in software that allow access to information or capabilities that can be used by a hacker as a stepping-stone into a system or network. The National Institute of Standards and Technology (NIST) uses a CERT advisory and whether or not a CVE identifier number has been issued as a guide to determine the severity of vulnerability, and classifies vulnerabilities into three levels in the ICAT Metabase [32], a predecessor of NVD.

Note that as severity metrics for vulnerabilities vary, depending on organizations, the Common Vulnerability Scoring System (CVSS) [33] was proposed as a common language with which to evaluate the severity of vulnerability in a comprehensive and general way in 2004.

4.8 Year 1999

(1) Starting to run hirt.hitachi.co.jp

In order to provide the Hitachi group with security information promptly and improve serviceability during planned outage for facility inspection at a business site, we set up an HIRT project main website (hirt.hitachi.co.jp) for internal use in December 1999.

(2) Investigation of website defacement

Website defacement had typically occurred since a webpage defacing occurred for the first time in the US in 1996 until the network worm era started (2001 - 2004). We conducted a survey on webpage defacing from 1999 to 2002 to find out how unauthorized access was made. (See Figure 14.)

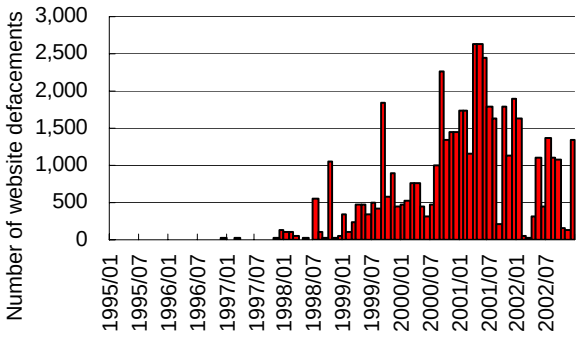


Figure 14: Changes in the number of websites defacements

4.9 Year 1998

(1) Starting to provide HIRT security information

In April 1998, we started to provide information on security measures mainly using an internal mailing list and an internal website for HIRT projects. This information is based on the security information issued by CERT/CC, JPCERT/CC, and product vendors (Cisco, HP, Microsoft, Netscape, Sun Microsystems, etc.).

(2) Holding network security seminars

On June 25 - 26, 1998, we provided "Network security" training for Hitachi. During this training, an US security engineer who had also participated in the US Security Conference DEFCON [34] as a speaker served as an instructor.

5 Conclusion

Security incidents have now entered in a new phase in which signs or damage are not brought to public attention. Even in the presence of these new threats, we can still solve problems by using the abilities of each organization to observe, analyze and cope with situations systematically through collaboration.

Taking the situation surrounding these incidents into account, HIRT will promote proactive measures against vulnerabilities using an Information Security Early Warning Partnership, establish a partnership with other organizations so that IRTs can cooperate with each other to combat new threats, and establish a cooperative relationship that can improve proactive measures against incidents.

(January 29, 2008)

References

1) Symantec: The State of Spam, A Monthly Report - December 2007 (2007/12), http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/Symantec_Spam_Report_-_December_2007.pdf
2) Trend Micro Incorporated: "Great Threats from Web, Second Series" (2007/6), http://blog.trendmicro.co.jp/archives/24
3) NIST NVD (National Vulnerability Database), http://nvd.nist.gov/
4) Information-Technology Promotion Agency, Japan: How vulnerability-related information is reported, http://www.ipa.go.jp/ security /vuln/report/press.html
5) LAC Corporation: Attack Trend Analysis Report Vol. 9 (2007/11), http://www.lac.co.jp/business/sns/intelligence/report/20071101lac_report.pdf
6) CSIRT - Nippon CSIRT Association, http://www.nca.gr.jp/
7) WARP (Warning, Advice and Reporting Point), http://www.warp.gov.uk/
8) NTT-CERT (NTT Computer Security Incident Response and Readiness Coordination Team), http://www.ntt-cert.org/
9) P2P Network Observation Using a Crawling Method, Information Processing CSEC Research Report Vol. 2007 No. 48. (2007/5)
10) Investigation Results of Information Leakage Caused by File Exchange Software in 2007 http://www.hitachi.com/hirt/publications/hirt-pub07012/metrics.html
11) @police: Description of Security: How to Use Websites Providing Information on Vulnerability Measures http://www.cyberpolice.go.jp/column/explanation21.html
12) CERT Advisory CA-2002-03, "Multiple Vulnerabilities in Many Implementations of the Simple Network Management Protocol (SNMP)" (2002/2), http://www.cert.org/advisories/CA-2002-03.html
13) Information-Technology Promotion Agency, Japan: Providing 2006 Security Implementation Course for Web Application Developers, http://www.ipa.go.jp/ security /vuln/event/200612.html
14) GlobalSign Adobe Certified Document Services, http://www.globalsign.com/adobe-cds/metrics.htm
15) CSIRT (Computer Security Incident Response Team); CSIRT activities in Hitachi (2006/5), http://www.microsoft.com/japan/technet/ security /secnews/columns/column060525.mspx
16) Proposal of RSS Extension for Security Information Exchange (2006/6), http://www.first.org/conference/2006/program/presentations.html - p198
17) FIRST (Forum of Incident Response and Security Teams), http://www.first.org/
18) Ministry of Economy, Trade and Industry, Notification No. 235: Standard for Handling Information Related to Vulnerabilities in Software, etc., http://www.meti.go.jp/policy/net security /downloadfiles/vulhandlingG.pdf
19) Information-Technology Promotion Agency, Japan: Information Security Early Warning Partnership Guideline, http://www.ipa.go.jp/ security /ciadr/partnership_guide.html
20) JVN (JP Vendor Status Notes), http://jvn.jp/
21) NISCC: NISCC Vulnerability Advisory 006489/H323: Vulnerability Issues in Implementations of the H.323 Protocol,

http://www.cpni.gov.uk/docs/re-20040113-00387.pdf?lang=en
22) Organization for Internet Safety: Draft Security Vulnerability Reporting and Response Process (2003/7), http://www.oisafety.org/resources.html
23) Information-Technology Promotion Agency, Japan: Materials on Policies for Releasing Security Vulnerability Information (2003/9), http://www.ipa.go.jp/ security /awareness/vendor/vulnerability200309012.pdf
24) LAC Co.: Policies for Reporting and Releasing Vulnerability Information (2003/8), http://www.lac.co.jp/business/sns/intelligence/SNSadvisory/SNSpolicy.html
25) CERT/CC Vulnerability Disclosure Policy, http://www.cert.org/kb/vul_disclosure.html
26) US-CERT: Vulnerability Note VU#459371: Multiple IPsec implementations do not adequately validate authentication data", http://www.kb.cert.org/vuls/id/459371
27) Considerations on Building JPCERT/CC Vendor Status Notes DB, CSS2002 (2002/10), http://jvn.doi.ics.keio.ac.jp/nav/CSS02-P-97.pdf
28) Building JVN that Supports Circulation of Security Information(2005/5), http://www.sdl.hitachi.co.jp/japanese/people/jvn/
29) CERT/CC Vulnerability Notes Database, http://www.kb.cert.org/vuls
30) CERT/CC Vulnerability Note Field Descriptions, http://www.kb.cert.org/vuls/html/fieldhelp
31) CVE (Common Vulnerabilities and Exposures), http://cve.mitre.org/
32) ICAT, http://icat.nist.gov/
33) CVSS (Common Vulnerability Scoring System), http://www.first.org/cvss/
34) DEFCON, http://www.defcon.org/