Global Information Assurance Certification Paper

Collection and Dissemination of Computer and Internet Security Related Information (Alerts, Advisories, Incident Notes, Vulnerability Notes, Summaries and other Bulletins**)**

Scott Fox

Version 1.2e

Introduction

Ongoing advances in technology and the growth of the Internet are introducing not only an increase in the number of vulnerabilities being found, but also an increase in the complexity of system administration, incident handling and forensic analysis work. There have been progressive changes in intruder techniques, increased difficulty of detecting an attack, increased amounts of damage, and an increased difficulty in catching the attackers. As a global Internet community we should increase our knowledge of where to turn for reliable up-to-date security information and trusted guidance. For a better understanding of how computer and Internet security information is collected, and then disseminated, we should frequent the Web sites of trusted CERT organizations, product vendors and the government. From here, let's go back to the beginnings of the first computer emergency response team.

Some history of the first computer emergency response team

[Northcutt] describes the sequence of events that started on November 2, 1988, when Robert Morris Jr., a graduate student in Computer Science at Cornell, wrote an experimental, self-replicating, self-propagating program called a *worm* and injected it into the Internet. He chose to release it from MIT, to disguise the fact that the worm came from Cornell. Morris soon discovered that the program was replicating and re-infecting machines at a much faster rate than he had anticipated – there was a bug. Ultimately, many machines around the country either crashed or became catatonic. When Morris realized what was happening, he contacted a friend at Harvard to discuss a solution. Eventually, they sent an anonymous message from Harvard over the network, instructing programmers how to kill the worm and prevent re-infection. However, because the network route was clogged, this message did not get through until it was to late. Computers were affected at many sites, including universities, military sites, and medical research facilities.

Following the Internet *worm* incident, which brought 10 percent of the Internet systems to a halt in November 1988, the Defense Advanced Research Projects Agency (DARPA) charged the Software Engineering Institute (SEI) with setting up a center to coordinate communication among experts during security emergencies and to help prevent future incidents. SEI is a federally funded research and development center at Carnegie Mellon University in Pittsburgh, Pennsylvania. From this incident emerged a small computer emergency response team, the first of its kind, created November 17th, 1988. This original computer emergency response team is known today simply as, CERT® Coordination Center or the CERT/CC. Since inception, the CERT/CC has helped to establish other response teams and more than 90 response teams around the world have adapted their incident handling practices [CERT/CC (1)].

Forum of Incident Response and Security Teams (FIRST)
[CERT/CC (1)] refers to FIRST as being founded in 1990, and a coalition of individual incident response teams that span major regions of globe. Each response team establishes trust with other response teams within the FIRST community, by forming contacts and developing working relationships. These relationships enable response teams to be sensitive to the diverse needs, technologies and policies of their constituents, being that FIRST is comprised of incident response teams from government, commercial, and academic organizations. While the CERT® Coordination Center was one of the 11 founding members, there are currently over 90 teams that belong to FIRST. A current list is available at http://www.first.org/team-info/. Some of the FIRST incident response teams maintain Web sites with resources for computer and Internet security related information, including security advisories and more.

Collection and Dissemination of Information
There are various ways the CERT® Coordination Center collects and disseminates computer and Internet security related information. Some of the information is reported to the CERT/CC by hotline telephone calls at (412) 268-7090 and via email at cert@cert.org. There's also a CERT Incident Handling Team and a Vulnerability Handling Team that are responsible for collecting and disseminating information as noted below. Additionally, components of the CERT *Knowledgebase*: the *Automated Incident Reporting Form* (AIR-CERT) and the *Interactive Incident Reporting Form* (IIRF) contribute to the collection of information.

The Incident Handling Team receives reports related to computer security from sites connected to the Internet. The team looks at the number of attacks attempted, probes, scans, compromises, denial-of-service and other incident criteria. They determine the method of the attack and the tools used by the intruder, as well as, the scope and magnitude of the attack. They analyze the findings and correlate this data with other reports, as well as the *Vulnerability Handling Team*, to determine what to report to the Internet community. The Incident Handling Team maintains the *CERT® Incident Notes* that describe current intruder activities that have been reported to the CERT/CC.

The Vulnerability Handling Team receives vulnerability reports from the public sources, trusted research teams and product vendors. The team then verifies and analyzes the reports for the validity, affect, systems affected, the exploits availability, and the frequency that the vulnerability is being exploited. They will work with other vulnerability reporters, product vendors and Internet experts to better understand the vulnerability, as well as, develop countermeasures and fixes or workarounds. The Vulnerability Handling Team maintains the public-accessible CERT/CC *Vulnerability Notes* database that contains *CERT® Incident Notes* and *Vendor Information* documents at http://www.kb.cert.org/vuls/. The team also maintains the ***restricted-access*** *Vulnerability Reports Catalog* at https://www.kb.cert.org/vulcatalog that is part of a central repository known as the CERT *Knowledgebase*.

In addition to the Vulnerability Reports Catalog, the CERT Knowledgebase contains Automated Incident Reporting (AIR-CERT) and the Interactive Incident Reporting Form (IIRF) for enhancing the collection of Internet information. Automated Incident Reporting (AIR-CERT) is a project involving the placement of sensors on the networks of various Internet-based organizations to monitor and log security events and anomalies. The AirCERT system is being developed using open source and low-cost components. To read more about AirCERT go to http://www.cert.org/kb/aircert/. The Interactive Incident Reporting Form (IIRF) is a web-based interactive form to report a security incident. The form contains a series of questions about your computer security incident that should be filled out as completely as possible. All of the information you submit remains confidential between you and the CERT/CC. The web site uses Secure Sockets Layer (SSL) 40-bit encryption that your browser must support. To view the Interactive Incident Reporting Form (IIRF) go to https://irf.cc.cert.org/. To subscribe to the CERT/CC and receive CERT® Advisories and CERT® Summaries, send e-mail to majordomo@cert.org and in the body of the message type: subscribe cert-advisory
Additionally, the publications by CERT® Coordination Center listed below are available on the World Wide Web at http://www.cert.org/ and can also be viewed at the USENET newsgroup: comp.security.announce.

Publications by CERT® Coordination Center or the CERT/CC
The publications by the CERT® Coordination Center are the backbone of providing computer and Internet security information to the Internet community. To better understand the information being disseminated by the CERT/CC, a detailed description of the advisory, incident note, vulnerability note and summaries are below.

- *CERT® Advisories* – *CERT® Advisories* are documents that address Internet security problems. They offer an explanation of the problem, information that helps you determine if your site has the problem, fixes or workarounds, and vendor information. *CERT® Advisories* are limited to vulnerabilities that meet a certain security threshold. Among the criteria for developing an advisory are the urgency of the problem, potential impact of intruder exploitation, and the existence of a software patch or workaround. It is difficult to establish a metric ranking the severity of a vulnerability that is appropriate for all systems. For instance, a severe vulnerability in a rarely used application might not qualify for a *CERT® Advisory*. In this case, *CERT® Vulnerability Notes* provide the means of publishing information about these less severe vulnerabilities. CERT/CC assigns each *CERT® Advisory* a unique ID number that is prefixed with "CA#". Some of the information fields that primarily make up *CERT® Advisories* are listed below.

    - ***CERT Advisory ID#***
    - ***Advisory Name***
    - ***Systems Affected***
    - ***Overview***

- ***Description***
- ***Impact***
- ***Solution***
  - *Vendor Information*
  - *Supplemental Information*
  - *References*
- ***Good Practices***
  - *Vendor Information*
- ***References***
- ***Author(s)*** *(Credit)*

On the day a *CERT® Advisory* is released, the CERT/CC sends it out to their mailing list, posts it to the USENET newsgroup comp.security.announce and makes it available on the CERT Web site at http://www.cert.org/advisories/. The statistics for the total number of security alerts published (1988-Q2, 2001): **333**. The first and second quarter of this year (Q1, Q2, 2001), **17** security alerts were published. Security alerts include *CERT® Advisories* and *CERT® Summaries*.

- *CERT® Incident Notes* – *CERT® Incident Notes* describe current intruder activities that have been reported to the CERT/CC incident response team. As of the writing of this paper, the CERT/CC lists **35** *CERT® Incident Notes*. Incidents are reported to the CERT/CC by hotline calls and via e-mail. *CERT® Incident Notes* are assigned a unique ID number that is prefixed with "IN#" and contain some of the fields that make up the *Vulnerability Notes*, as well as some others. Here is a list of the fields that primarily make up *CERT® Incident Notes*.

  - ***Incident Note ID#***
  - ***Incident Name***
  - ***Systems Affected***
  - ***Overview***
  - ***Description***
  - ***Mitigation***
  - ***Impact***
  - ***Solutions***
  - ***Reporting***
  - ***Author(s)*** *(Credit)*

  The statistics of the total number of incidents reported to CERT/CC for (1988-Q2, 2001): **63,187**. The first two quarters of this year alone (Q1, Q2, 2001), **15,476** incidents were reported.

- The CERT/CC *Vulnerability Notes* database contains two types of documents. *CERT® Vulnerability Notes*, which generally describe vulnerabilities independent of a particular vender, and *Vendor Information* documents, which are links to information about a specific vendor's solution to a problem. *CERT® Vulnerability Notes* are similar to *CERT® Advisories*, but may describe less severe vulnerabilities, contain less complete information or affect a smaller number of systems. The vulnerability ID number for all of the documents in the CERT/CC *Vulnerability Notes* database is prefixed with "VU#", fully indexed and CVE

compliant (*Common Vulnerabilities and Exposures*). An explanation of CVE is given further down. At the time of the writing this paper, the public-access database contains **194** *Vulnerability Notes*. The CERT/CC also has a restricted-access *Vulnerability Reports Catalog* that contains descriptive and referential information regarding more than 1,300 vulnerabilities reported to the CERT® Coordination Center. Statically, the total number of vulnerabilities reported for (1995-Q2, 2001): **3,747**. While the first two quarters of this year alone (Q1, Q2, 2001), **1,151** vulnerabilities were reported.

CERT ® Vulnerability Notes – Here is a list and description of the fields that make up *CERT® Vulnerability Notes* [CERT/CC (3)].

Vulnerability ID# – ID number randomly assigned by CERT/CC to uniquely identify a vulnerability. ID's are four to six digits long and have a prefix of "VU#".
Vulnerability Name – A short description that summarizes the nature of the problem and the affected software product.
Overview – An abstract of the vulnerability that provides a summary of the problem and its impact to the reader.
Description – One or more paragraphs of text describing the vulnerability.
Impact – describes the advantage that an intruder might gain by exploiting the vulnerability and may list necessary preconditions the attacker must meet.
Solution – Contains information about how to correct the vulnerability in general terms.
Systems Affected – Includes a list of vendors who may be affected by the vulnerability and links to more detailed information. **(**The more detailed information is the *Vendor Information* documents that are described below**)**.
References – A collection of URLs providing additional information about the vulnerability.
Credit – Acknowledges the individuals who report the vulnerabilities and the CERT/CC authors.
Date Public – Date on which the vulnerability was first known to the public, to the best of CERT/CC's knowledge and/or by default, their vulnerability note publication date.
Date First Published – Date when CERT/CC first published the vulnerability note.
Date Last Updated – Date the vulnerability note was last updated due to new information in a particular field.
CERT Advisory – If a CERT Advisory was published for this vulnerability, this field will contain a pointer to that advisory.
CVE Name – The CVE name is the 13 character ID used by the "Common Vulnerabilities and Exposures" group to uniquely identify a vulnerability. The CVE Name field is also a link to the CVE web site with additional information. **(**While the mapping between CVE names and CERT/CC vulnerability ID's are usually pretty close, in some cases multiple vulnerabilities may map to one CVE name, or vice versa**)**. The CVE group tracks a large number of security problems, not all of which meet CERT/CC's criteria for being considered vulnerability. For instance, the CERT/CC does not track viruses or Trojan horse programs in the *Vulnerability Notes* database.
Metric – The metric value is a number between 0 and 180 that assigns an approximate severity to the vulnerability. This number considers several factors, including:

- Is information about the vulnerability widely available or known?
- Is the vulnerability being exploited in the incidents reported to the CERT/CC?
- Is the Internet Infrastructure at risk because of this vulnerability?
- How many systems on the Internet are at risk from this vulnerability?
- What is the impact of exploiting the vulnerability?
- How easy is it to exploit the vulnerability?
- What are the precautions required to exploit the vulnerability?

These questions are answered with approximate values that may differ significantly from one site

to another so users should not rely too heavily on the metric for prioritizing vulnerabilities.
Document Revision – Contains the revision number for this document.

Vendor Information – Here is a list and description of the fields that make up *Vendor Information* [CERT/CC (3)].

Date Notified – Date that the CERT/CC notified the vendor of the vulnerability, or the date that the vendor first contacted the CERT/CC, or the earliest date when the vendor is known to have been aware of the vulnerability.
Date Modified – As vendors produce patches and publish advisories, the *Vendor Statement* or the *CERT/CC Addendum* fields get updated and then this date is changed.
Status Summary – Indicates in broad terms whether the vendor has any products that the CERT/CC considers to be vulnerable. Users should also read the detailed vendor statements.
Vendor Statement – The vendor's official response to the CERT/CC queries about the vulnerability. This information is provided directly by the vendor and does not necessarily reflect the CERT/CC opinions.
CERT/CC Addendum – One or more paragraphs of text from the CERT/CC commenting on this vulnerability and may disagree with the vendor statement or assessment of the problem.

The CERT/CC *Vulnerability Notes* database can be sorted and viewed by *Name*, *ID Number*, *CVE Name*, *Date Public*, *Date Updated* and *Severity Metric*.

- *CERT® Summaries* – The CERT/CC issues the CERT *Summary* each quarter to make aware the types of attacks reported to the CERT/CC incident response team over the past three months. Additionally, other pertinent incident and vulnerability information, as well as, pointers to other resources of information are noted. *CERT® Summaries* are sent to their mailing list, posts them to the USENET newsgroup comp.security.announce and makes them available on the CERT web site at http://www.cert.org/summaries/.

Common Vulnerabilities and Exposures (CVE)
CVE is a list of information security vulnerabilities and exposures that aims to provide common names for publicly known problems; CVE is not a vulnerability database. CVE only contains the standard name, a brief description, and references to related documents. CVE is designed to make it easier to share data across separate vulnerability databases and security tools with this "common enumeration." To search for CVE and Candidates go to http://cve.mitre.org/cve/ where there are currently over **1,500** total entries listed. CVE is the result of a collaborative effort of representatives from numerous security-related organizations such as security tool vendors, academic institutions, and government, as well as other prominent security experts. The support for CVE is evident with the labeling of "CVE-Compatible" products and security tools. To be "CVE-Compatible" implies that a Web site, database, security tool or other security product is: CVE searchable, the output information includes the CVE name(s), and that the provider has used CVE names accurately in the product. To view a list of the organizations that has declared or is working to make their product/database "CVE-

Compatible" go to http://cve.mitre.org/compatible/index.html.

Our SANS GIAC training is "CVE-Compatible" due to student assignments of several courses referencing CVE. Also worth mentioning is the "CVE-Compatible" ICAT Metabase available at http://icat.nist.gov/icat.cfm. ICAT indexes the information available in CERT advisories, ISS X-Force, Security Focus, NT Bugtraq, Bugtraq, and a variety of vendor security and patch bulletins. ICAT does not compete with publicly available vulnerability databases but instead is a search engine that drives traffic to them. ICAT is maintained by the National Institute of Standards and Technology.

The Big Picture

The Internet Software Consortium has conducted an Internet Domain Survey twice a year since 1987 [ISC (1)]. They attempt to discover every host on the Internet by doing a complete search of the Domain Name System. The survey methodology changed in January 1998, due system administrators blocking DNS zone transfers for security reasons, to the "new" survey method of using ordinary DNS queries. The new survey results are considered to be an estimate of the minimum size of the Internet. With the latest survey results from January 2001 showing more than **190** million hosts as advertised in the DNS [ISC (2)]. This type of Internet survey helps to bring things into perspective with regard to the activity, threat and survivability of the Internet. Certainly, the collection and dissemination of computer and Internet security information is essential for survival with such diverse user demographics; including government agencies, academic and research institutions, corporate users and home users.

References

[Northcutt] Northcutt, Stephen. *Information Assurance Foundations: Core Issues and Challenges*. SANS GIAC Level One GSEC.

[CERT/CC (1)] CERT® Coordination Center or the CERT/CC. *Meet the CERT® Coordination Center*.
http://www.cert.org/meet_cert/meetcertcc.html

[CERT/CC (2)] CERT® Coordination Center or the CERT/CC. *Overview Incident and Vulnerability Trends*.
http://www.cert.org/present/cert-overview-trends/

[CERT/CC (3)] CERT® Coordination Center or the CERT/CC. *CERT/CC Vulnerability Note Field Descriptions*
http://www.kb.cert.org/vuls/html/fieldhelp

[FIRST] Forum of Incident Response and Security Teams
http://www.first.org/about

[CVE (1)] Common Vulnerabilities and Exposures.
http://www.cve.mitre.org/

[CVE (2)] Common Vulnerabilities and Exposures. *Frequently Asked Questions*
http://www.cve.mitre.org/about/faq.html

[ICAT] Computer Security Division at the National Institute of Standards and Technology. *ICAT Metabase*.
http://icat.nist.gov/icat.cfm

[ISC (1)] Internet Software Consortium.
http://www.isc.org/

[ISC (2)] Internet Software Consortium. *Internet Domain Survey, January 2001*
http://www.isc.org/ds/WWW-200101/index.html