CERT® Coordination Center 1994 Annual Report

January 1995

CERT Division

This material is based upon work funded and supported by the Department of Defense under Contract No. FA8702-15-D-0002 with Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center.

The view, opinions, and/or findings contained in this material are those of the author(s) and should not be construed as an official Government position, policy, or decision, unless designated by other documentation.

References herein to any specific commercial product, process, or service by trade name, trade mark, manufacturer, or otherwise, does not necessarily constitute or imply its endorsement, recommendation, or favoring by Carnegie Mellon University or its Software Engineering Institute.

This report was prepared for the

SEI Administrative Agent
AFLCMC/AZS
5 Eglin Street
Hanscom AFB, MA 01731-2100

DM17-0052

Table of Contents

1 Activities and Services

From January through December 1994, the CERT Coordination Center received 29,580 e-mail messages and 3,664 hotline calls reporting computer security incidents or requesting information.

The CERT staff handled 2,241 computer security incidents during this period. The following chart provides a by-month break-out of this activity. There have been over 40,241 sites affected by these incidents. (22,650 of these sites were involved in a failed sendmail attack, where all computers within a specified IP address range were probed to exploit an old sendmail vulnerability.) Based on current computer security incident data, the following are the top four techniques for exploiting Internet hosts:

- Sniffer attacks: reusable passwords, Trojan utilities
- Email related: 3 different sendmail attacks
- Network File System (NFS) attacks
- Network Information Services (NIS) attacks

1.1 Advisories

Fifteen advisories were released in 1994. The first advisory, released February 3, was a response to a dramatic increase in network monitoring by intruders, who were capturing passwords and installing "back doors" for future access to systems. The monitoring had been under way previously, but reports of the network monitoring attacks increased in a single week from a few isolated reports to indications that tens of thousands of systems may have been compromised. The advisory provided both a short-term workaround for the problem and recommendations for a long-term solution, including a discussion of one-time passwords. Follow-up activities have continued. Unlike most security incidents, this one received extensive attention from the media, prompting information requests from people who had not previously been involved with the CERT Coordination Center.

In addition, the CERT team notified an archive site that their software being readied for distribution had been modified. The inconsistency became apparent when the team checked MD5 checksums prior to releasing them in the advisory. CERT members brought the problem to the attention of the archive site, who investigated and discovered that one of the machines had been broken into and a Trojan horse installed in the patched program. They were able to take immediate action, averting a potentially very wide distribution of the Trojan horse.

A complete listing of the advisories issued during 1994 can be found in Appendix A.

1.2 Vendor Bulletins

In December, the CERT Coordination Center began publishing vendor-initiated bulletins. These bulletins contain verbatim text from vendors describing security problems and their solutions. Our goal is to help the vendors' security information get wide distribution quickly. We distribute CERT vendor-initiated bulletins the same way as CERT advisories. People who are on the CERT mailing list and who read the comp.security.announce newsgroup automatically get bulletins as well as advisories. CERT staff will continue to publish advisories on critical security problems. Bulletins are an additional way of distributing information, not a replacement for advisories. The first bulletin, VB-94:01, distributed information from The Santa Cruz Operation and the second, VB-94:02, from Digital Equipment Corporation. A complete listing of the vendor bulletins issued during 1994 can be found in Appendix B.

2 Information Services

2.1 Security Improvement Program (SIP)

CERT members have been developing a networked information technology security taxonomy and questionnaire in collaboration with the Software Engineering Institute's Risk Program. They completed two formal field test profiles, one with a commercial corporation and the second with a division of a government agency.

The profile itself will be a "report card" identifying security issues as they relate to the client organization's environment. The profile can be used to assist sites in making strategic decisions regarding improvement activities. The profile is not a "certification" or evaluation of the site. It is intended as a mutual learning experience in which the site can gain insights about its strengths and weaknesses, and CERT staff can learn some more about the state of the practice in specific industries.

With a site profile as a starting point, this program provides practical guidance in addressing the issues and shortcomings that were identified during the development of the profile. The objective is to start a site on an improvement path in a way that ensures a high probability of success. Information Requests We have received approximately 1,230 requests for information that are security related, but not necessarily related to a particular incident or advisory.

There were 1,545 sites that have asked to be added to either our advisory, tools, or course mailing lists.

3 Research and Development

3.1 CERT 2000

The CERT 2000 project is a short-term design effort with the goal of producing a high-level optimized redesign of CERT functionality, roles, and processes. Our objective is to create the best high-level data-oriented design for the coordination center's current (and projected) functionality and expertise.

This high-level design will be used as starting point for evolving the center to a more scalable and manageable organization. It will also serve as a foundation for the implementation process for automating appropriate elements of CERT functionality. To accomplish this goal, we will build upon the CERT-Information Management System data gathering and analysis effort that has taken place over the past several months.

As our procedures and tools are refined, it is our intent to share them with other members of the Forum of Incident Response and Security Teams (FIRST).

4 Advocacy & Community Support

The CERT Coordination Center staff members were invited to give presentations at several conferences, workshops, and meetings during 1994. This has been found to be an excellent tool to educate attendees in the area of network information system security and Incident Response. In addition to formal presentations, CERT members continue to present "Birds of a Feather" sessions and participate in panel presentations. 4.1 Advocacy On March 22, Dain Gary was one of five experts who testified at the Internet Security Hearing before the Subcommittee on Science U.S. House of Representatives. The purpose of the hearing was to enable the subcommittee to evaluate the status of security on the Internet today, examine measures currently available to enhance security, assess the effectiveness and degree of implementation of these measures, and identify obstacles to enhancing Internet security.

Jim Ellis is the General Chair for The Internet Society Symposium on Network and Distributed System Security to be held in San Diego, California on February 16-17, 1995. The symposium is intended for those interested in the more practical aspects of network and distributed system security, focusing on actual system design and implementation, rather than in theory.

Barbara Fraser was invited to be a member of an advisory group, the Electronic Grants Initiative Subcommittee of the Division of Research Grant's (DRG) Advisory Board. The DRG is developing an electronic grant application technology and the four advisory group members will help evaluate the DRG electronic initiatives. The advisory board will offer advice in terms of what is technologically available and feasible now for the extension to the broad community of organizations and investigators that seek support from NIH. Specifically, Fraser has been asked to participate to identify security issues and to provide guidance in this area. The first subcommittee meeting was held on November 8-9 in Bethesda, Maryland.

Moira West-Brown attended a computer crime statistics working group at the National Institute of Standards and Technology (NIST) in November. This group is developing standard terms to describe security incidents to facilitate the creation of a national database of computer crime data.

The coordination center staff also published two papers to raise the awareness of the network community about security issues. "CERT Incident Response and the Internet," by Kathy Fithen and Barbara Fraser, was published in the August 1994 issue of Communications of the ACM. "Keeping Intruders Away," by Jim Ellis, Barbara Fraser, and Linda Pesante, appeared in the September issue of UNIX Review. In addition, the most recent issue of Bridge (#1 1994) contained an article, "Secure Software Reuse," describing the joint work of the CERT team and the National Security Agency.

The Sixth Annual Computer Security Incident Handling Workshop was held in Boston, MA on July 25-29. The workshop was cosponsored by the Forum of Incident Response and Security Teams (FIRST), the CERT Coordination Center, Digital Equipment Corporation, and the National Institute of Standards and Technology (NIST). The focus of this year's workshop was on tools for incident handling in an international arena. In addition to participating on various panels, CERT staff led three sessions: Incident Handling Teams Status and Update, Nontraditional and Public Domain Network Servers, and Interoperability in the FIRST Community. Tom Longstaff was chair of the program committee for the conference. 4.2 Internet Engineering Task Force - IETF Barbara Fraser is chairing two working groups for the Internet Engineering Task Force (IETF): the Site Security Handbook (SSH) Working Group, and the Guidelines and Recommendations for Incident Processing (GRIP) Working Group. The SSH group is producing two documents, a site security handbook for system and network administrators, and one for users. The GRIP group is producing guidelines for security incident response teams and technology vendors. Barbara is also a member of the Security Directorate and attending those meetings as well.

Barbara Fraser and Carter Bullard hosted the first meeting of the CERT Technical Council during the Toronto Internet Engineering Task Force meeting. This group will provide technical expertise to the CERT Coordination Center when we are working with particularly difficult problems.

Appendix A

CA-94:01 Ongoing Network Monitoring Attacks
All systems that offer remote access through rlogin, telnet, and ftp are at risk. The advisory includes a description of the activity and suggested approaches for addressing the problem.

CA-94:02 Revised Patch for SunOS /usr/etc/rpm.mountd Vulnerability
A vulnerability is present in SunOS 4.1, 4.1.1, 4.1.2, and 4.1.3 /usr/etc/rpc.mountd. Unauthorized remote hosts will be able to mount the file system. The advisory describes how to obtain a patch for the problem from Sun.

CA-94:03 AIX Performance Tools Vulnerabilities
Vulnerabilities are present in the bosext1.extcmds.obj performance tools in AIX 3.2.5 and in those AIX 3.2.4 systems with Program Temporary Fixes (PTFs) U420020 or U422510 installed.

CA-94:04 SunOS /usr/ucb/rdist Vulnerability
This advisory addresses a vulnerability with /usr/ucb/rdist in SunOS 4.0.3, 4.1.1, 4.1.2, 4.1.3, and 4.1.3c on sun3 and sun4 architectures. The advisory describes how to obtain a patch for the problem from Sun.

CA-94:05 MD5 Checksums
This advisory gives the MD5 checksums for a number of SunOS files, along with a tool for checking them.

CA-94:06 Writable /etc/utmp Vulnerability
This advisory addresses a vulnerability with /etc/utmp ins SunOS 4.1.X and Solaris 1.1.1 operating systems. Solbourne Computer, Inc. and other Sparc products using Sun OS 4.1.X or Solaris 1.1.1 are also affected. Solaris 2.x is not affected by this problem.

CA-94:07 wuarchive ftpd Trojan Horse
Warning about intruder-modified source for wuarchive ftpd, which introduced a Trojan horse in versions 2.2, 2.1f, and possibly earlier versions. Recommended solution is to upgrade to version 2.3.

CA-94:08 ftpd Vulnerabilities
This advisory addresses two vulnerabilities with some releases of fptd and announces new versions and patches to correct these problems. ftpd versions affected are wuarchive ftpd 2.0-2.3, DECWRL ftpd versions prior to 5.93, and BSDI ftpd version 1.1 prior to patch level 5.

CA-94:09 /bin/login Vulnerability
This advisory addresses a vulnerability in /bin/login of all IBM AIX 3 systems, and Linux systems. A workaround and patch information are included in this advisory.

CA-94:10 IBM AIX bsh Vulnerability
This advisory addresses a vulnerability in the batch queue (bsh) of IBM AIX systems running versions prior to and including AIX 3.2. The CERT staff recommends a workaround to disable the bsh feature. IBM provides a patch for systems requiring this functionality.

CA-94:11 Majordomo Vulnerabilities
This advisory addresses two vulnerabilities in Majordomo versions prior to 1.92. The CERT staff recommends installing version 1.92, but provides workarounds if this is not possible.

CA-94:12 Sendmail Vulnerabilities
This advisory addresses two vulnerabilities in sendmail (8): one in the debug option (-d) and other in the error message header option (-oE). Patch information is listed as of the date of advisory release. The CA-94:12.README file contains the most current list.

CA-94:13 SGI IRIX Help Vulnerability
This advisory addresses a vulnerability in the Silicon Graphics, Inc. IRIX 5.x Help system. SGI recommends installing the patch, but has provided a workaround to disable the Help system if this is not possible.

CA-94:14 Trojan Horse in IRC Client for UNIX
This advisory addresses a Trojan horse in some copies of ircII version 2.2.9, the source code for the Internet Relay Chat (IRC) client for UNIX systems. The Trojan Horse provides a back door through which intruders can gain unauthorized access to accounts of IRC users.

CA-94:15 NFS Vulnerabilities
This advisory addresses tools being used by intruders to exploit a number of NFS vulnerabilities. These tools are widely available and widely distributed. The impact varies depending on whichvulnerabilities are present. In the worst case, intruders gain unauthorized root access from a remote host.

A list of the 1994 CERT vendor-initiated bulletins that have been issued are as follows:

VB-94:01 SCO Advisory.
The programs at(C), login(M), prwarn(C) sadc(ADM), and pt_chmodmay each allow unauthorized root access to the system. There are four unrelated issues present, one for each program listed above.

VB-94:02 Digital Equipment Corporation
Potential security vulnerabilities exist where, under certain circumstances, user access or privilege may be expanded.