Software Engineering Institute
Carnegie Mellon University

CERT® Coordination Center 1998 Annual Report

January 1999

CERT Division

http://www.sei.cmu.edu

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.

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 Introduction

The CERT Coordination Center (CERT/CC) was formed by the Defense Advanced Research Projects Agency (DARPA) in November 1988 in response to the needs identified during an Internet security incident. Our charter is to work with the Internet community in detecting and resolving computer security incidents as well as taking steps to prevent future incidents. Our specific mission is to

- Provide a reliable, trusted, 24-hour, single point of contact for emergencies.
- Facilitate communication among experts working to solve security problems.
- Serve as a central point for identifying and correcting vulnerabilities in computer systems.
- Maintain close ties with research activities and conduct research to improve the security of existing systems.
- Initiate proactive measures to increase awareness and understanding of information security and computer security issues throughout the community of network users and service providers.

The CERT/CC is part of the Networked Systems Survivability (NSS) Program at the Software Engineering Institute (SEI), Carnegie Mellon University. The primary goal of the NSS Program is to ensure that appropriate technology and systems management practices are used to resist attacks on networked systems and to limit damage and ensure continuity of critical services in spite of successful attacks. Our main areas of activity for 1998 were survivable network management practices, survivable network technology, security incident handling, vulnerability analysis, and information services

We develop and publish security improvement practices that provide concrete, practical guidance that helps organizations improve the security of their networked computer systems. These practices are published as security improvement modules and focus on best practices that address important problems in network security.

We recently completed pilots of an information security evaluation method that helps organizations identify their security needs. CERT/CC staff members assessed the security of organizations' networks and presented their results to each organization's management. These results provided a foundation for an ongoing security improvement program. Development is now under way for a self-evaluation method that builds on what we learned during our pilot. Self-evaluations will give organizations a comprehensive, repeatable technique they can use to identify vulnerabilities in their networked systems and keep up with changes over time. The method takes into consideration policy, management, administration, and other organizational issues, as well as technology, so organizations can gain a comprehensive view of the state of their systems' security.

Because security improvement is an ongoing process within an organization, we are developing an adaptive security management process that builds on and incorporates our work on security practices and security self-evaluations. The adaptive process presents a structure that organizations can use to develop and execute a plan for continuously improving the security of their networked systems.

In the area of survivable network technology, the CERT/CC is concentrating on the technical basis for identifying and preventing security flaws and for preserving essential services if a system is penetrated and compromised. Approaches that are effective at securing bounded systems (systems that are controlled by one administrative structure) are not effective at securing unbounded systems such as the Internet. Therefore, the technical approaches include design and implementation strategies, recovery tactics, strategies to resist attacks, survivability trade-off analysis, and the development of security architectures. Drawing on our vast collection of incident data, our researchers are creating usage scenarios and intruder scenarios that will be used to identify the points in an architecture that are both essential to an organization's mission and susceptible to attack. This provides the basis for a method for analyzing network technology. Also under way is development of a simulator for modeling and predicting the survivability attributes of systems while they are under development, preventing costly vulnerabilities before the system is built.

We hold an annual Information Survivability Workshop to foster cooperation and collaboration between domain experts and the survivability research community to improve the survivability of critical, real-world systems. The 1998 workshop, "Protecting Critical Infrastructures and Critical Applications" was organized by the CERT/CC and the Software Engineering Institute and sponsored by the IEEE Computer Society

Incident response activities include developing an infrastructure that is effective at improving Internet-connected systems' resistance to attack as well as detecting and resolving attacks on those systems. Our primary concern is identifying and resolving high-impact threats and vulnerabilities, such as

- attacks on network infrastructure
- widespread or automated attacks
- attacks that involve new vulnerabilities, techniques, tools

Our ongoing computer security incident response activities help the Internet community deal with its immediate problems while allowing us to understand the scope and nature of the problems and of the community's needs. Our understanding of current security problems and potential solutions comes from this first-hand experience with compromised sites on the Internet and subsequent analysis of the security incidents, intrusion techniques, configuration problems, and software vulnerabilities.

To increase awareness of security issues and help organizations improve the security of their systems, we continue to disseminate information through multiple channels:

- telephone and email
  hotline: +1 412 268-7090
  email: cert@cert.org
  mailing list: cert-advisory-request@cert.org
- USENET newsgroup: comp.security.announce
- World Wide Web: http://www.cert.org/

2 Highlights of CERT/CC Activities and Services

2.1 Incident Response

From January through December 1998, the CERT/CC received 41,871 email messages and 1,001 hotline calls reporting computer security incidents or requesting information. We received 262 vulnerability reports and handled 3,734 computer security incidents during this period. More than 18,990 sites were affected by these incidents

When a security breach occurs, the CERT/CC incident response staff helps affected sites to identify and correct problems in their systems and to develop system safeguards and security policies. We coordinate with other sites affected by the same incident and, when an affected site explicitly requests, we facilitate communication with law enforcement and investigative agencies

When we receive a vulnerability report, CERT/CC vulnerability experts analyze the potential vulnerability, working with technology producers and vendors. We advise them of security deficiencies in their products, help them to resolve the problems, and facilitate the distribution of corrections to other response teams and to the Internet community at large.

2.1.1 Intruder Activity

Below we describe some of the most serious intruder activities reported to the CERT/CC in 1998

1. **Growth and evolution of automated scanning tool**

   The CERT/CC has received reports of intruders executing widespread attacks using scripted tools to control a collection of information-gathering and exploitation tools. This activity was reported throughout the year in a number of CERT/CC alerts (CA-97.26, CS-98.01, CS-98.03, CS-98.07, CS-98.08, IN-98.01, IN-98.02, IN-98.04, IN-98.05, IN-98.06). The combination of functionality used by the scripted tools enables intruders to automate the process of identifying and exploiting known vulnerabilities in specific host platforms. In the past year, the CERT/CC has come to recognize two new approaches to scanning: the stealth scan and scanning to identify system or network architecture. The stealth scans appear to have a common goal: to gather information about target sites while avoiding detection by using techniques that might be overlooked by intrusion detection systems and system administrators. By scanning to identify system or network architecture, intruders are employing scanning techniques to identify the operating system used by a particular host and/or to determine information about the structure of the target network.

2. **statd**

   The vulnerability in statd continues to be exploited. First reported by the CERT/CC in CA-97.26, statd activity is referenced in CS-98.01 and CS-98.03. statd provides network status monitoring. It interacts with lockd to provide crash and recovery functions for the locking services on NFS. Due to insufficient bounds checking on input arguments which may be supplied by local users or remote users, it is possible to overwrite the internal stack space of the statd program while it is executing a specific rpc routine. By supplying a carefully designed input argument to the statd program, intruders may be able to force statd to execute arbitrary commands as the user running statd. In most instances, this is root. This vulnerability may be exploited by local users. It also can be exploited remotely without the intruder requiring a valid local account if statd is accessible via the network.

3. **named**

   Intruders are increasingly scanning networks for machines running vulnerable versions of named. This was reported in CS-98.04 and CS-98.05. This increased activity in named is consistent with trends that the CERT/CC has seen with previous vulnerabilities; in these cases, intruders have launched widespread scans to look for machines running vulnerable IMAP servers or web servers with the phf vulnerability, and then exploited the vulnerability on those machines. While we have had many reported incidents involving the exploitation of named, at least one incident appears to involve widespread attacks against authoritative domain name servers.

4. **mountd**

   Intruders exploited a vulnerability in some implementations of the software that NFS servers use to log requests to use file systems. Activity around this vulnerability was noted in CA-98.12 and CS-98.08. The vulnerability lies in the software on the NFS server that handles requests to mount file systems. This software is usually called mountd or rpc.mountd. Intruders gained administrative privilege to the vulnerable NFS file server. This vulnerability can be exploited remotely and does not require an account on the target machine. On some vulnerable systems, the mountd software is installed and enabled by default

2.1.2 FedCIRC

The CERT/CC incident response team is part of FedCIRC, the Federal Computer Incident Response Capability. FedCIRC provides incident response and other security-related services to Federal civilian agencies. It was established in 1996 as a pilot effort of the National Institute of Standards and Technology (NIST), the CERT/CC, and the Computer Incident Advisory Capability (CIAC). As of October 1, 1998, FedCIRC

is managed by the General Services Administration (GSA) and operated by the CERT/CC.

The CERT/CC participates in the FedCIRC seminar series. Seminar topics included "How to Establish an Incident Response Capability" and "Establishing a Computer Forensic Analysis Program." CERT/CC staff also led a FedCIRC Workshop on WWW security and incident trends. The attending staff members fielded questions regarding how the CERT/CC handles vulnerabilities and how it determines if advisories will be written.

More information about FedCIRC (including guidelines for reporting an incident) is available at http://www.fedcirc.gov or by calling the FedCIRC Management Center at (202) 708-5060

2.2 Incident and Vulnerability Analysis

Our ongoing computer security incident response activities help the Internet community deal with its immediate problems while allowing us to understand the scope and nature of the problems and of the community's needs. Our understanding of current security problems and potential solutions comes from this first-hand experience with compromised sites on the Internet and subsequent analysis of the security incidents, intrusion techniques, configuration problems, and software vulnerabilities.

We have become a major reporting center for incidents and vulnerabilities because we have an established reputation for discretion and objectivity. Organizations trust us with sensitive information about security compromises and network vulnerabilities because we have proven our ability to keep their identities and information confidential. Our connection with the Software Engineering Institute and Carnegie Mellon University contributes to our ability to be neutral, enabling us to work with commercial competitors and government agencies without bias. As a result of the community's trust, we are able to obtain a broad view of incident and vulnerability trends and characteristics.

When we receive a vulnerability report, CERT/CC vulnerability experts analyze the potential vulnerability and work with technology producers to inform them of security deficiencies in their products and to facilitate and track their response to these problems. We interact with more than 50 vendors, as well as developers of freely available software such as sendmail and BIND. Vendors often provide information to the CERT/CC for inclusion in advisories. We summarize that information in an appendix for the benefit of the vendors' customers.

Another source of vulnerability information comes from incident analysis. Repeated incidents of the same type often point to the existence of a vulnerability and, often, the existence of public information or automated tools for exploiting the vulnerability.

To achieve long-term benefit from vulnerability analysis, we have begun to identify the underlying software engineering and system administration practices that lead to

vulnerabilities and, conversely, practices that prevent vulnerabilities. We will broadly disseminate this information to practitioners and consumers and influence educators to include it in courses for future software engineers and system administrators. Only when software is developed and installed using the defensive practices will there be a decrease in the expensive, and often haphazard, reactive use of patches and workarounds.

2.3 Publications

2.3.1 Advisories

The CERT/CC published 13 advisories in 1998. Among the criteria for developing an advisory are the urgency of the problem, potential impact of intruder exploitation, and existence of a software patch or workaround. On the day of release, we send advisories to a mailing list, post them to the USENET newsgroup comp.security.announce and make them available on the CERT Web site at http://www.cert.org/.

To keep advisories current, we update them as we receive new information. The complete listing of advisories issued during 1998 can be found in Appendix A.

2.3.2 Vendor-Initiated Bulletins

CERT vendor-initiated bulletins contain verbatim text from vendors describing security problems and their solutions. Through these bulletins, we help the vendors' security information get wide distribution quickly. The bulletins are distributed through the same channels as advisories.

Thirteen bulletins were published in 1998. Appendix B contains a complete listing.

2.3.3 CERT Summaries

We publish the CERT Summary as part of our ongoing efforts to disseminate timely information about Internet security issues. Eight summaries were issued in 1998. Two of those issues were special editions describing widespread, large-scale attacks. The primary purpose of the summary is to call attention to the types of attacks currently being reported to the CERT/CC. Each summary includes pointers to advisories or other publications that explain how to deal with the attacks. Summaries are distributed the same way as advisories and bulletins.

2.3.4 Incident and Vulnerability Notes

The CERT/CC also began publishing two new web documents in 1998: Incident Notes and Vulnerability Notes. We created the "notes" as an informal means for giving the Internet community timely information relating to the security of its sites. Incident Notes describe current intruder activities that have been reported to the CERT/CC incident response team. Vulnerability Notes describe weaknesses in Internet-related systems that could be exploited but that currently do not meet the criteria for advisories. Appendix C and D contain a complete listing

2.3.5 Survivable Network Management Practices

Four sets of practices are currently available on the CERT web site and in hard copy: *Detecting Signs of Intrusion; Preparing to Detect Signs of Intrusion; Security for Information Technology Service Contracts;* and *Security for a Public Web Site.*

Four more sets of practices are under way: *Responding to Signs of Intrusion; Securing Desktop Workstations; Securing Network Servers; Selecting, Installing,*and *Operating Firewalls and Intrusion Detection Systems.*

2.3.6 Survivable Network Technology

Information on Survivable Network Technology activities is available in the following research papers available on the CERT web site: *Survivable Network Systems: An Emerging Discipline; A Case Study in Survivable Network System Analysis;* and *Requirements Definition for Survivable Network Systems.*

2.3.7 Other Security Information

The CERT/CC captures lessons learned from incident handling and vulnerability and makes them available to users of the Internet through a web site archive of security information and products. These include answers to frequently asked questions, a security checklist, "tech tips" for systems administrators, and security tools such as Tripwire, MD5, and TCP wrappers.

In addition, we developed and published Incident Reporting Guidelines. This document (available on the CERT web site) outlines suggested steps for reporting incidents to the CERT/CC, as well as suggestions for responsible handling of incidents.

2.4 Media Exposure

Internet security issues increasingly draw the attention of the media. The headlines, occasionally sensational, report only a small fraction of the events that are reported to the CERT/CC. Even so, accurate reporting on security issues can raise the awareness of a broad population to the risks they face on the Internet and steps they can take to protect themselves. Ultimately, the increased visibility of security issues may lead consumers to demand increased security in the computer systems and network services they buy.

In the course of a year, the CERT/CC is referred to in most major U.S. newspapers and in a variety of other publications, from the *Chronicle of Higher Education* to *IEEE Computer*. Our staff gives interviews to a selected number of reporters, under the guidance of the SEI public affairs manager.

This year, the CERT/CC was referenced in a variety of publications including *The San Jose Mercury News, The New York Times, PCWeek, PC Magazine, Information Security, Pittsburgh Post-Gazette, Software Magazine, Network Computing,* and

online publications such as *WIRED News, CNN Financial Network, CNET News, Cipher,* and *The Net Vital Survey*.

A CERT/CC staff member was interviewed by National Public Radio (NPR). The story focused on the denial-of-service attacks targeting Windows 95/NT machines. CERT/CC staff also participated as guest panelists on National Public Radio news programs discussing Internet security.

Another staff member was featured as part of a segment ("Waging War with Computers") on the *CBS Evening News*. The piece focused on the susceptibility of government computers to attack.

The *Lehrer News Hour* featured CERT/CC operations in a computer security story.

2.5 Training

CERT/CC staff provides access to ongoing training to improve the skills of incident response teams and individuals charged with information security responsibilities through seminars and courses. These offerings provide pragmatic information needed to develop an incident response capability and are based on CERT/CC experience. Training for managers of incident response teams includes topics such as team communication, interacting with the media, balancing workload, and setting priorities. Topics for the technical staff include detecting and responding to incidents, intruder trends and attack patterns, analyzing vulnerabilities, and policies and planning. Specific types of incidents are included, such as those involving NT, the World Wide Web, and cgi-bin scripts. This training is interactive, including role-playing to give participants experience in applying the instruction. Courses offered in 1998 included the following:

Incident Handling for Managers
Internet Security for Managers
Internet Security for System and Network Administrators
Managing Computer Security Incident Response Teams (CSIRTs)
Computer Security Incident Handling for Technical Staff (Introduction)

2.6 Advocacy and Other Interactions with the Community

The CERT/CC has the opportunity to advocate high-level changes that improve Internet security and network survivability. Additionally, CERT/CC staff members are invited to give presentations at conferences, workshops, and meetings. These activities enhance the understanding of Internet security and incident response issues.

2.6.1 Protecting the Internet Infrastructure

In a January 1997 report to the President's Commission on Critical Infrastructure Protection (PCCIP), the CERT/CC outlined the effect of a successful, sustained attack on

the Internet for critical national infrastructures such as telecommunications, banking and finance, emergency services, and the information infrastructure itself. The concerns raised there continue to be influential and guide our work in this area.

The CERT/CC assigns a higher priority to incidents and vulnerabilities that directly effect the Internet infrastructure. Toward that end, CERT/CC staff monitors reports closely for incidents that indicate a threat to infrastructure sites such as network service providers and Internet service providers. Similarly, domain name servers and routers receive close attention as vital infrastructure components. We also regularly review incident and vulnerability data for threats to the operation of widely used technology like the WWW and prevalent applications like NT, Solaris, sendmail, and Java. We also look closely at the activity reported by major archive sites and other computer security incident response teams.

In addition to its incident response work, CERT/CC staff attended and participated in a number of discussions centered around critical infrastructure protection. CERT/CC technical staff is actively involved in planning security improvements to the Domain Name Service, on which all Internet users depend. We have met with Network Solutions, Inc. and the Internet Assigned Numbers Authority (IANA), who are charged with managing much of the domain name system, and are active in the Internet Society, which also influences change in the Internet.

2.6.2 Internet Engineering Task Force

Members of our staff influence the definition of Internet protocols through participation in the Internet Engineering Task Force (IETF); a member of our staff sits on the Security Area Advisory Group to ensure that the CERT/CC perspective is brought to bear on all new standards activities.

2.6.3 Internet Architecture Board

A CERT/CC staff member was one of 25 participants in an Internet Advisory Board (IAB) Security Architecture Workshop held in 1998. The primary goal of that workshop was to identify what Internet security mechanisms are available, and when they can, should, or must be used. Among the topics discussed were short-term guidelines for IETF working groups on improving consideration of security issues and, for the long term, an Internet security "architecture."

The IAB was established in 1983 and is a technical advisory group of the Internet Society. The IAB consists of 13 voting members. Six of the members are nominated by the IETF. The IAB exists to serve and help the IETF, attempting to strike a balance between action and reaction.

2.6.4 Forum of Incident Response and Security Teams (FIRST)

Members of the CERT/CC participated in the 10th FIRST Conference. CERT/CC staff helped lead the event (a CERT/CC member was re-elected to the chair of the

group's steering committee). CERT/CC staff made presentations and participated in discussions with other attendees representing government, academia, and private industry. The conference drew attendees from 16 nations. The committee, which has always included a representative from the CERT/CC, meets quarterly and holds teleconferences each month in which there is no meeting.

A current list of FIRST members is available from http://www.first.org/team-info/. As of January 1999, 77 teams belong to FIRST and membership applications for additional teams are pending.

2.6.5 Vendor Relations

CERT/CC has continued to work closely with technology producers to inform them of security deficiencies in their products and to facilitate and track their response to these problems. Staff members have worked to influence the vendors to improve the basic, as shipped, security within their products and to include security topics in their standard customer training courses. We interact with more than 50 vendors, as well as developers of freely available software such as sendmail and BIND.

Vendors often provide information to the CERT/CC for inclusion in advisories. We summarize that information in an appendix for the benefit of the vendors' customers.

2.6.6 Visitors

Among our visitors this year were representatives from AUSCERT (Australian incident response team), ASSIST (Department of Defense incident response team), MXCERT (Mexican incident response team), and Mr. Steve Orlowski, special advisor on information technology security policy, Australian Attorney-General's Office. These visits enhance understanding of Internet security and incident response issues and promote mutual trust and cooperation that are essential for effective response to international incidents.

Other visitors included Dr. Ann Miller, Deputy Assistant Secretary of the Navy; Mr. Dick Clark, Special Assistant to the President for National Security Affairs and Senior Director of Global Issues; Mr. Jeffrey Hunker; director, Critical Infrastructure Assurance Office; and Mr. Bob Nemetz, director, Office of the Secretary of Defense Studies & FFRDC programs. These visits provide an additional means by which to obtain feedback and direction with our sponsoring organization.

2.6.7 External Events

CERT/CC staff members were invited to give presentations at conferences, workshops, and meeting during 1998. This has been found to be an excellent tool to edu-

cate attendees in the area of network information system security and incident response. Transition efforts included involvement in conferences and meetings such as the examples listed below:

- Second Annual INFOSEC Defensive Information Operations Workshop
- Network Security Information Exchange
- The Second Workshop on Education in Computer Security
- Seventh Annual USENIX Security Symposium
- Joint Information Assurance Tools Working Group
- DARPA Intrusion Detection Principle Investigators Workshop
- National Cybercrime Training Partnership
- Joint Information Assurance Operations Working Group
- Second National Colloquium for Information Systems Security
- National Institute of Health Information Technology Security Conference
- Third International Conference on Requirements Engineering
- National Security Telecommunications Advisory Committee
- Annual policy forum hosted by former U.S. Senator Sam Nunn
- Crime Prevention Association of Western Pennsylvania
- Association of Old Crows Information Warfare Conference
- The Information Security Education Training and Professionalization Working Group (INFOSEC ETAPWG)
- Information Assurance Vulnerability Action Working Group
- Department of Defense Information Assurance Conference Office of the Secretary of Defense - Education, Training, and Awareness Policy Working Group
- Twenty-first National Information Systems Security Conference
- 1998 Information Environment for the Future Conference
- 1998 Conference on Maritime Technology
- Y2K Database Working Group
- The Second Information Survivability Workshop - Protecting Critical Infrastructures and Critical Applications
- National Telecommunications Infrastructure Vital Issues Process Meeting (sponsored by National Communication System and Sandia National Laboratories)
- Infrastructure Protection Conference

Appendix A: CERT Advisories Published in 1998

The following advisories were published in 1998. We update the advisories as necessary. Advisories are available on the CERT Web site at http://www.cert.org/advisories/.

CA-98.01 "smurf" IP Denial-of-Service Attacks

Both the intermediary and victim of this attack may suffer degraded network performance both on their internal networks or on their connection to the Internet. Performance may be degraded to the point that the network cannot be used.

A significant enough stream of traffic can cause serious performance degradation for small and mid-level ISPs that supply service to the intermediaries or victims. Larger ISPs may see backbone degradation and peering saturation.

CA-98.02 Vulnerabilities in CDE

Local users are able to gain write access to arbitrary files. This can be leveraged to gain privileged access.

Local users may also be able to remove files from arbitrary directories, thus causing a denial of service.

CA-98.03 Vulnerabilities in ssh-agent

When connecting to the AF_UNIX socket, the SSH client runs as super-user, and performs insufficient permissions checking. This makes it possible for users to trick their SSH clients into using credentials belonging to other users. The result is that any user who uses RSA authentication AND uses ssh-agent, is vulnerable. Attackers can exploit this vulnerability to access remote accounts belonging to the ssh-agent user.

CA-98.04 Microsoft Windows-based Web Servers unauthorized access-long file names

Users are able to gain unauthorized access to files protected solely by the web server.

CA-98.05 Multiple Vulnerabilities in BIND

Topic 1: A remote intruder can gain root-level access to your name server.

Topics 2 and 3: A remote intruder is able to disrupt normal operation of your name server.

CA-98.06 Buffer Overflow in NIS+

Depending on the configuration of the target machine, a remote intruder can gain root access to a vulnerable system or cause the NIS+ server to crash, which will affect the usability of any system which depends on NIS+.

Additionally, if your NIS+ server is running in NIS compatibility mode and if an intruder is able to crash the NIS+ server, the intruder may be able to masquerade as an NIS server and gain access to machines that depend on NIS for authentication. Finally, if an intruder is able to crash an NIS+ server and there are clients on the local network that are initialized by broadcast, an intruder may be able to provide false initialization information to the NIS+ clients. Clients that are initialized by hostname may also be vulnerable under some circumstances.

CA-98.07 Vulnerability in Some Usages of PKCS#1

Under some circumstances, an intruder who is able to observe an SSL-encrypted session, and subsequently interrogate the server involved in the session, may be able to recover the session key used in that session and then recover the encrypted data from that session.

CA-98.08 Buffer overflows in some POP servers

Remote users can gain privileged (root) access to systems running vulnerable versions of POP servers.

CA-98.09 Buffer Overflow in Some Implementations of IMAP Servers

Remote intruders can execute arbitrary commands under the privileges of the process running the vulnerable IMAP server. If the vulnerable IMAP server is running as root, remote intruders can gain root access.

CA-98.10 Buffer Overflow in MIME-aware Mail and News Clients

An intruder who sends a carefully crafted mail message to a vulnerable system can, under some circumstances, cause code of the intruder's choosing to be executed on the vulnerable system. Additionally, an intruder can cause a vulnerable mail program to crash unexpectedly. Depending on the operating system on which the mail client is running and the privileges of the user running the vulnerable mail client, the intruder may be able to crash the entire system. If a privileged user reads mail with a vulnerable mail user agent, an intruder can gain administrative access to the system.

CA-98.11 Vulnerability in ToolTalk RPC Service

Due to an implementation fault in rpc.ttdbserverd, it is possible for a malicious remote client to formulate an RPC message that will cause the server to overflow an automatic variable on the stack. By overwriting activation records stored on the stack, it is possible to force a transfer of control into arbitrary instructions provided by the attacker in the RPC message, and thus gain total control of the server process.

CA-98.12 Remotely Exploitable Buffer Overflow Vulnerability in mountd

This vulnerability affects NFS servers running certain implementations of mountd, primarily Linux systems. On some systems, the vulnerable NFS server is enabled by default. This vulnerability can be exploited even if the NFS server does not share any file systems.

CA-98.13 Vulnerability in Certain TCP/IP Implementations

Intruders can disrupt service or crash systems with vulnerable TCP/IP stacks. No special access is required, and intruders can use source-address spoofing to conceal their true location. By carefully constructing a sequence of packets with certain characteristics, an intruder can cause vulnerable systems to crash, hang, or behave in unpredictable ways. This vulnerability is similar in its effect to other denial-of-service vulnerabilities, including the ones described in CA-97.28 (Teardrop_Land).

Appendix B: CERT Vendor-Initiated Bulletins Issued in 1998

The following vendor-initiated bulletins were published in 1998. Vendors publish many more bulletins than these. The CERT vendor-initiated bulletins contain vendor information that particularly warrants the widespread dissemination that CERT/CC provides.

VB-98.01 CGI Security Hole in EWS1.1

In situations where the web server is running under a user-id with sufficient access privileges, a hacker could conceivably cause damage to the host system. Because a search entered by a user into the web page is passed as command line argument to the search binary, and because the command line is interpreted by the shell before the search binary is invoked, it is possible for a hacker with sufficient know-how to craft a search that could cause commands embedded in the search string to be invoked on the host system.

VB-98.02 Apache Security Advisory

It is possible to create a sequence of data such that a buffer overflow occurs while cfg_getline is reading from a file. If someone has access to create any of these types of files on the server, this hole is generally exploitable to gain full access to the user Apache runs as. There are several coding problems in mod_include that may result in a buffer overflow or in the child process going into an infinite loop. By sending many requests with a large number of '/'s in to a server, it is possible to cause a large amount of CPU time to be used in processing these requests. Making multiple simultaneous requests of this nature could result in a high load average, high CPU usage, and possibly starving other processes for CPU resulting in a denial of service attack. In some cases, it may be possible for a remote user who has control of a DNS server to return a hostname specifically designed to exploit a coding hole in logresolve. It is possible to deliberately create a listing that will cause Apache to dump core ...it would be possible to use this to create a denial of service attack that would render the server effectively inoperative. When caching is enabled in mod_proxy, Apache writes cached files to disk as the user that the server runs as. If an attacker can gain access to this user id (eg. by running a CGI script from a pre-existing account on the machine) then they can modify the filenames on disk resulting in a buffer overflow.

VB-98.03 IRIX 6.3 & 6.4 mailcap vulnerability

If the user is a privileged or root user, the "Trojan horse" System Manger Task will execute with root privileges and can lead to a root compromise.

VB-98.04 Vulnerabilities in xterm and Xaw

By crafting an arbitrarily long string that contains embedded machine code and using it to set specific "resources," a user may obtain a shell prompt that

has root privileges.

VB-98.05 PIX Private Link Key Processing and Cryptography Issues

If attackers know the details of the key-parsing error in the PIX Private Link software, they will know 8 bits of the key ahead of time. This reduces the effective key length from the attacker's point of view from 56 to 48 bits. This reduction of the effective key length reduces the work involved in a brute-force attack on the encryption by a factor of 256. That is, knowledgeable attackers can, on the average, find the right key 256 times faster than they would be able to find it with a true 56-bit key.

VB-98.06 File Access Issue with Internet Information Server

Web clients that connect to IIS can read the contents of any NTFS file in an IIS v-root directory to which they have been granted "read access." They can read these files even if the file is marked for "applications mappings," such as used with Active Server Pages scripts.

VB-98.07 OpenVMS (VAX & ALPHA) V7.1 LOGINOUT Potentiial Security Vulnerability

A potential vulnerability with LOGINOUT for OpenVMS (VAX & ALPHA) V7.1 software has been discovered, where under certain circumstances, a user may gain unauthorized access.

VB-98.08 Cisco IOS Remote Router Crash

An error in Cisco IOS software makes it possible for untrusted, unauthenticated users who can gain access to the login prompt of a router or other Cisco IOS device, via any means, to cause that device to crash and reload.

VB-98.09 CRM Temporary File Vulnerability

Users who have access to the computer on which CRM is installed may gain access to information which gives them unauthorized access to the managed routers and switches. This affects both Solaris and Windows NT systems.

VB-98.10 Security Vulnerabilities in "mscreen" Serial Multiscreens Utility

Security vulnerabilities have been discovered in the SCO "mscreen" serial multiscreens utility. The vulnerabilities could allow local users to gain root privileges. An exploit script for one of the vulnerabilities has been published, so we recommend that the patch described below be installed on all affected systems as soon as possible. Users who have access to the computer on which CRM is installed may gain access to information which gives them unauthorized access to the managed routers and switches. This affects both Solaris and Windows NT systems.

VB-98.11 Cisco IOS Command History Release at Login Prompt

An error in Cisco IOS software makes it possible for untrusted, unauthenticated users who can gain access to the login prompt of a router or other Cisco

IOS device, via any means, to obtain fragments of text entered by prior interactive users of the device. This text may contain sensitive information, possibly including passwords. This vulnerability exposes only text entered at prompts issued by the IOS device itself; the contents of data packets forwarded by IOS devices are not exposed, nor are data entered as part of outgoing interactive connections, such as TELNET connections, from the IOS device to other network nodes.

VB-98.12 Update available for "Untrusted Scripted Paste" Issue in Microsoft Internet Explorer 4.01

Microsoft has released a patch that fixes a vulnerability involving scripted pastes that has been discovered with Internet Explorer 4.01 on Win32 and Win16 platforms. The vulnerability could make it possible for a malicious hacker to create a web site that, when visited, is able to use script to read a file on the user's system. The file must be in a location known to the malicious hacker. This has also been referred to as the "Cuartango" vulnerability.

VB-98.13 Cisco IOS DFS Access List Leakage

Errors in certain Cisco IOS software versions for certain routers can cause IP datagrams to be output to network interfaces even though access lists have been applied to filter those datagrams. This applies to routers from the Cisco 7xxx family only, and only when those routers have been configured for distributed fast switching (DFS).

Appendix C: CERT Incident Notes Issued in 1998

The following Incident Notes were published in 1998. Incident Notes describe current intruder activities that have been reported to the CERT/CC incident response team.

IN-98.01 Scans to Port 1/tcpmux and unpassworded SGI accounts

Intruders are using one automated tool to scan for IRIX machines and another to telnet to those that have tcpmux. They are gaining unauthorized access to accounts that do not have passwords. In some cases, a root compromise is possible.

IN-98.02 New Tools Used For Widespread Scans

A new intruder tool is in widespread use to scan networks for many different vulnerabilities:

- statd - This vulnerability permits attackers to gain root privileges. It can be exploited by local users. It can also be exploited remotely without the intruder requiring a valid local account if statd is accessible via the network.
- IMAP/POP3 - Remote users can obtain root access on systems running a vulnerable IMAP or POP server. They do not need access to an account on the system to do this.
- IRIX accounts without passwords
- BIND - Depending on which vulnerability is exploited, a remote intruder can gain root-level access to your name server or can disrupt normal operation of the name server.
- cgi-bin vulnerabilities, including phf, handler, and test-cgi - Impact varies. Some CGI scripts allow an attacker to execute arbitrary commands on a WWW server under the effective user-id of the server process. Other vulnerabilities allow a remote user to retrieve any world readable files, execute arbitrary commands and create files on the server with the privileges of the httpd process which answers HTTP requests. This may be used to compromise the HTTP server and under certain configurations gain privileged access. In other cases, arbitrary commands can be executed with httpd daemon privileges, and depending on configuration of the HTTP server, privileged access may be possible.
- NFS filesystems exported to everyone - Intruders can read any file on the system.
- X11 (open X servers) - Intruders can monitor keystrokes and mouse events, thus learning what users do in their interactions with the compromised system.

IN-98.03 Password Cracking Activity

An intruder collected a list of 186,126 accounts and encrypted passwords. At the time the password file collection was discovered, the intruder had successfully guessed 47,642 of these passwords by using a password-cracking tool. Some of the password files included information identifying the site where the file originated. The collection is reported to contain entries from at least one password file that was originally shadowed.

IN-98.04 Advanced Scanning

Intruders are using advanced scanning techniques to gain information about organizations' networks, including a scan that is likely to avoid detection. They can gain information about the structure of the network, the operating systems, and type of TCP/IP stacks. They can use this information to optimize attacks and to identify targets that have particular vulnerabilities.

IN-98.05 Probes with Spoofed IP Addresses

Reports indicate that intruders have spoofed IP addresses to conduct scans similar to those discussed in previous CERT/CC advisories (CA-98.09, CA-97.09). At first, these probes apppeared to be ordinary IMAP scans. After further investigation, most of these sites determined that another compromised host on the same network was the true origin of the IMAP scan. It's possible that the intruder was able to run a network sniffer to capture the results of these probes.

IN-98.06 Automated Scanning and Exploitation

The CERT Coordination Center has received reports of intruders executing widespread attacks using scripted tools to control a collection of information-gathering and exploitation tools. The combination of functionality used by the scripted tools enables intruders to automate the process of identifying and exploiting known vulnerabilities in specific host platforms.

IN-98.07 Windows NT "Remote Explorer" Virus

Recently, a Windows NT virus by the name of "Remote Explorer" or "RICHS" has received public attention. Although this virus can modify files, our interaction with Microsoft leads us to believe that this virus is unable to gain any privileges beyond those of the user running the infected program. That is, the virus has only the capabilities, file permissions, etc., of the person running it. However, Remote Explorer also can install itself as a Windows NT service if an infected file is run by someone with local administrator privileges. Once it has been installed as a service, Remote Explorer can impersonate anyone else who subsequently logs into the system, including domain administrators. Then, using the privileges of a domain administrator, Remote Explorer attempts to self-propagate by infecting other files on the network.

Appendix D: CERT Vulnerability Notes Issued in 1998

The following Vulnerability Notes were published in 1998. Vulnerability Notes describe weaknesses in Internet-related systems that could be exploited but that do not currently meet the criteria for advisories.

VN-98.01 Vulnerabilities in the XFree86 Distribution of the xterm Program and Xaw Library

An unprivileged user with access to the local system can gain root access to the system.

VN-98.02 Kernel Modification

If the kernel has been modified by an intruder, it may be difficult or impossible to establish trust in that system. Functions provided by the kernel (and programs relying on those functions) will act in the manner described by the intruder. If an intruder modifies the kernel, it is as if the intruder has installed an operating system of his choice.

VN-98.03 WinGate IP Laundering

The default configuration for WinGate allows an intruder to use a WinGate server to conceal his or her true location without the need to forge packets. Intruders can use WinGate to effectively launder their IP addresses during an Internet-based attack. A victim of an attack using a WinGate server is only able to trace the connection back to the WinGate server. Additionally, a site running a vulnerable WinGate server may be implicated in a security incident when in fact an intruder has used the WinGate server to conceal his or her true location.

VN-98.04 The Year 2000 Problem

Software errors due to the Y2K problem may severely affect your ability to operate normally. A great deal has already been published about the Year 2000 Problem; this document merely provides pointers to other sources of information.

VN-98.05 Cisco PIX Firewall "established" Command

Under certain conditions, including the use of static conduits and the established command, an intruder can establish a connection to an arbitrary port on a host protected by a firewall if any port on that host is reachable via a static conduit.

VN-98.06 Microsoft Internet Explorer Jscript Bulnerability

If an Internet Explorer user visits a web site that includes Javascript. Maliciously designed to exploit this vulnerability, the script may be able to run arbitrary code on the user's machine.

VN-98.07 Back Orifice

Because it is a Trojan horse, users must install Back Orifice themselves or be tricked into installing it. It can be disguised in a variety of ways and is ostensibly positioned as a "remote administration tool." Once the Trojan horse is on the user's system, the client (which may be running anywhere on the Internet) can access the affected system with the privileges of the user who inadvertently installed it.

VN-98.08 Two Independent Vulnerabilities in ufsrestore and ufsdump

There are two independent vulnerabilities in both the ufsrestore and ufsdump utilities included in some versions of SunOS. Both vulnerabilities allow a user with a local account to obtain unauthorized root access. Intruders that have access to a local account can leverage these vulnerabilities to gain unauthorized root access.