U.S. DOE's Computer Incident Advisory Capability

CIAC NOTES

Number 01 January 31, 1994

With this issue, the United States Department of Energy's Computer Incident Advisory Capability (CIAC) begins the electronic publication of articles on relevant computer security topics — CIAC Notes. This is a service requested by our customers and we welcome your feedback on this issue of CIAC Notes. Please contact the editor, Allan L. Van Lehn, CIAC, 510-422-8193 or send E-mail to ciac@llnl.gov.

Table of Contents

What is CIAC Notes?

CIAC has published urgent advisories and important information bulletins since its inception in 1988 to alert sites about threats and attacks or to report vulnerabilities and their countermeasures. CIAC Notes, a third level of notification, is a means to communicate information that does not warrant the issuing of a bulletin nor fit the bulletin format. It is for timely, but not time-critical information; it includes articles with either a broader scope or with more depth than can be covered in a bulletin. CIAC Notes will be published as needed, without a schedule and distributed only electronically. This issue, being the first, is probably larger and has more background information than ones to follow. All the articles in this issue were provided by CIAC team members. If you have information appropriate for this forum, please let us know. CIAC advisories, bulletins and notes are available electronically from CIAC's computer security information servers, Felicia and Irbis. Instruction on accessing these servers is provided in the article: *CIAC Computer Security Information Servers*, below.

Subscribing to CIAC Notes

We intend to use electronic methods only to distribute CIAC Notes. Our mailing list is managed by a public domain software package called ListProcessor which supports several types of user commands via E-mail. Our Internet address is: ciac-listproc@llnl.gov. ListProcessor ignores E-mail header subject lines, so you may leave that blank.

To subscribe to CIAC Notes (i.e., be added to our mailing list), send the following request as the E-mail message body, substituting vaild information for items in parentheses:

subscribe CIAC-NOTES (Full_Name) (Phone_number)

To subscribe (add an address which is) a distribution_list, first subscribe the person responsible for your distribution_list. You will receive an acknowledgement, containing your address and access_code, with information on how to change information, cancel the subscription, or get help. Then, change the address to be the distribution_list address by sending a second E-mail request. As the body of the message, send the following request:

set CIAC-NOTES address (access_code) (distribution_list_address)

To be removed from this mailing list, send the following request:

unsubscribe CIAC-NOTES

For more information, send the following request:

help

If you have any questions about this list, you may contact the list's owner: listmanager@cheetah.llnl.gov

The New CIAC Project Leader

We are pleased to announce that Sandra L. Sparks is the new CIAC Project Leader. Sandy brings fifteen years of a professional background in computer science, the last several years working in computer security areas, and lots of enthusiasm to her role in CIAC. Sandy is available to talk with you via phone at 510-422-6856 or E-mail as ssparks@llnl.gov. In an emergency incident situation, she can be contacted via the secondary skypage: call 1-800-SKYPAGE (759-7243) and enter PIN number 855-0074.

The CIAC Team

The following people are presently assigned to the CIAC Team. Each one has a variety of computer security experience and various specializations.

Name	Technical Support Areas
Cindy Durflinger	Administrative support specialist
Rich Feingold	OpenVMS, ULTRIX, UNIX, PC, networks, training
Bill Orvis (half time)	DOS, Macintosh, UNICOS, OpenVMS, engineering
Karyn Pichnarczyk	DOS, Macintosh, viruses, UNIX
Sandy Sparks	IBM VM/CMS, PC systems
Allan Van Lehn	OpenVMS, sys admin, special projects, Notes editor
Steve Weeber	SunOS, UNIX, X-windows, firewalls, Netmap

Contacting CIAC

If you require additional assistance or wish to report a vulnerability, call CIAC at 510-422-8193, fax messages to 510-423-8002 or send E-mail to ciac@llnl.gov. For emergencies and off-hour assistance, call 1-800-SKYPAGE (759-7243) and enter PIN number 855-0070 (primary) or 855-0074 (secondary). The CIAC Duty Officer, a rotating responsibility, carries the primary skypager. The Project Leader carries the secondary skypager. If you are unable to contact CIAC via phone, please use the skypage system.

The Growing Threat of Automated Intrusion

The term *computer hacker*, often used by the media today to describe computer intruders, was originally used to describe people that enjoyed exploring the details of computer systems, finding undocumented or unintended features. These people were often called wizards or gurus, in deference to the collection of arcane knowledge they possessed. Most malicious intruders were also willing to spend days pouring over source code, but they were looking for vulnerabilities and persistently examining machine after machine looking for weaknesses. They tended to share their discoveries with others of like intent, often over the network they explored as if it were a giant computer maze game.

This characterization of the average computer intruder is rapidly changing. More and more of today's *hackers* aren't investing the time to master complex operating systems or develop contacts in the computer underground. This new breed of intruder simply makes use of an increasing number of publicly available, automated intrusion tools. The obscure knowledge required to exploit system vulnerabilities has now been encoded in easy-to-use, widely available software packages. The information that in the past was available only to a determined few is now easily accessible by anyone. This represents a dramatic increase in the size of the potential intruder population and a corresponding increase in the level of threat to which systems are exposed.

A recent example of one such tool, the Internet Security Scanner (ISS), was described in CIAC Advisory D-25. ISS was made publicly available on the Internet in late September, and within hours of its release, CIAC received multiple reports of attempted ISS intrusions. The tool automatically scans a specified range of network addresses, testing each machine found for the presence of more than a dozen vulnerabilities. ISS then generates a report summarizing the methods by which each machine may be compromised. This new tool reduces to a single command a process that in the past would have required detailed knowledge, programming skills, and persistence.

Now, more than ever, it is vital that hosts be configured securely and that networks be monitored for intruder activity. Tools, available to U.S. Government agencies from the Computer Security Technology Center at Lawrence Livermore National Laboratory, such as the Network Intrusion Detector (NID) and the Security Profile Inspector (SPI), are capable of both detecting automated attacks in progress and preventing their success.

For further information, contact Stephen A. Weeber, CIAC at 510-422-8193 or send E-mail to ciac@llnl.gov.

Virus Information

PC Virus Information

Boot sector type viruses are the most prevalent of the reported PC viruses in 1993. Of these, the top two are Form and Stoned. Hence, CIAC urges users to have *no diskettes* in the A drive during the boot up process. CIAC also encourages use of the capability some clone computers have to disable bootup from the A drive. Check the hardware manual to see if your computer has this capability and how to set it. Beware! Even if a diskette is not bootable, it can transfer a boot sector virus to the hard drive during the boot up process [unless bootup from the floppy drive(s) is disabled].

Current PC Anti-Virus Software

Reference to any specific commercial product does not necessarily constitute or imply its endorsement, recommendation or favoring by CIAC, the United States Government or the University of California. As of January 31, 1994, the current versions of PC anti-virus software are:

Product Name	Company	Version	Date released
AVP	Kami Limited	1.07	October 1993
CP AntiVirus (CPAV)	Central Point Software Inc.	2.1	November 1993
Data Physician PLUS! *	Digital Dispatch Inc.	4.0C	January 1994
FindVirus - Dr.Solomon's AntiVirus Toolkit	Ontrack Computer Systems Inc.	6.5	October 1993
F-PROT	FRISK Associates	2.10c	December 1993
IBM Antivirus	IBM Corp.	1.04	December 1993
Integrity Master	Stiller Research, Dept. B1	1.51	June 1993
Norton AntiVirus (NAV)	Symantec Corp.	3.0	October 1993
PC Rx Antivirus	Trend Micro Devices Inc.	2.65	?
SCAN	McAfee Associates	109	November 1993
Thunderbyte	?	6.09	?
Untouchable	Fifth Generation Systems Inc.	29.04	?
VET	Cybec	E7.334	?
Virex for the PC	Datawatch, Triangle Sw. Div.	2.91	October 1993
ViruSafe	EliaShim Microcomputers Inc.	5.3	?
VirusBuster	Leprechaun Sw. Int'l Ltd.	3.98	?

* Note: The Department of Energy has a site license for Data Physician Plus. It is available from your site CPPM.

To obtain further information, contact Karyn Pichnarczyk, CIAC, 510-422-8193 or send E-mail to ciac@llnl.gov.

A PC Virus: "The Satan Bug Virus"

The Satan Bug Virus represents a new generation of polymorphic, self-encrypting viruses. This virus is described in CIAC Bulletin D-22. CIAC has reports of it at three sites in the U.S., one site within and two others outside of the DOE. The virus infects programs (.COM, .EXE, and .OVL files) and drivers (.SYS files) on MS-DOS/PC-DOS computers. When an infected program is executed, the virus runs first, loads itself into memory and then runs the infected program. The only thing you might notice is that an infected program seems to load a little slower than normal. The virus then watches the operating system for file open requests (Open or Execute) and infects each opened file, if it is not already infected. It keeps track of which files are infected by adding 100 years to the file's modification date. This isn't obvious when listing a directory by using the DIR command because only the last two digits of the year are displayed.

Because the virus also attacks drivers, and drivers are often located in limited sized holes in high memory, an infected driver will often no longer fit into its hole. When that happens, the system will fail. Since drivers control access to networked file servers, a machine with the Satan Bug Virus may be unable to connect to a file server. This is a primary symptom of a Satan Bug Virus infection.

Satan Bug is not widespread, is not intentionally damaging, but does result in a loss of time and a loss of access to facilities especially while it is being removed. At the moment, most current versions of anti-viral programs detect and remove the virus (please see the list in the article *Current Virus Information* above). Be careful when scanning disks for viruses, if your scanner is infected, or if the virus is in memory and the scanner didn't detect it (or it did detect it and you told it to scan your disk anyway) the act of opening each file to scan for viruses may infect every file on your hard disk. If your scanner indicates that a virus is in memory, or that the scanner has been infected, *do not complete the scan*. Reboot your system from a clean, locked floppy disk, then run a clean version of the scanner on another locked floppy disk.

For further information, contact William J. Orvis, CIAC at 510-422-8193, or send E-mail to ciac@llnl.gov.

Macintosh Virus Information

Two new Macintosh viruses have recently been discovered, CODE-1 and MBDF-B. Neither appear intent on doing damage, but can cause system failures due to poor programming. New versions of Macintosh anti-virus software now detect and eradicate these viruses.

CODE-1's only explicit action is to rename the hard disk to "Trent Saburo" if the system is restarted on October 31 of any year. On any other day, the virus simply spreads. The MBDF-B virus is a simple variant of the MBDF-A virus. It has some of the same symptoms: Claris applications indicate that they have been altered; BeHierarchic shareware ceases to work properly; and some programs crash if a menu bar item is selected with the mouse. The MBDF-B virus is so similar to MBDF-A that some antivirus packages actually report MBDF-B as the MBDF-A virus.

Current Macintosh Anti-Virus Software

Reference to any specific commercial product does not necessarily constitute or imply its endorsement, recommendation or favoring by CIAC, the United States Government or the University of California. As of January 31, 1994, the current versions of Macintosh anti-virus software [all released early November 1993] are:

Product Name	Version	Comments
CPAV	3.0a	Central Point Software Inc. BBS: 503-690-6650
Disinfectant	3.3	Free Software
Gatekeeper	1.3	Free Software
Rival	CODE-1 Vaccine	E-mailed to all registered users
SAM Virus Clinic & Intercept	3.5.9	Symantec Customer Service 800-441-7234
Virex	4.1	Datawatch Corp., Triangle Sw. Div. 919-549-0711, BBS: 919-549-0042
VirusDetective	5.0.10	Shareware (product phasing out)

To obtain further information, contact Karyn Pichnarczyk, CIAC, 510-422-8193 or send E-mail to ciac@llnl.gov.

A Macintosh Virus: "The Merry Xmas Virus"

The Merry Xmas Virus, discovered at the end of 1992, infects Hypercard stacks on the Macintosh. The virus is written in Hypercard's scripting language and resides in the Stack script. Whenever a card is opened or closed, the virus checks to see if the current stack and the Home stack are infected. If either is not, the virus infects it. A symptom of the virus is many short disk accesses when you are not doing anything, as the virus continually tests the current stack for the infection. The virus is not intentionally damaging and does little more than copy itself from stack to stack. It can only infect the currently open stack and the Home stack. It does not infect stacks that are not open.

Some anti-virus utilities detect the virus in stacks that had the virus previously but have had it removed. They find remnants of the virus on a disk in unused portions of the disk file. These remnants cannot infect but are sufficient to set off some virus detection programs.

If you have a Hypercard Stack that has been reported as having the virus, you can check that stack by examining the Stack script. If at the end of the Stack script you find script comments of the form "-- merryxmas" at the ends of many of the lines, the stack is infected. Probably your Home stack is infected as well. To get rid of the virus, select the lines of virus code (about the last 54 lines of the script), delete them and save the script. Quickly switch to your Home stack's stack script and check it as well. Continue checking both the Home's and the stack's stack script until they both no longer have the virus, because as you are switching from one stack to the next, the virus may be reinfecting the stack you have just disinfected. Running Hypercard and the Home stack from a locked disk will prevent reinfection.

To obtain further information, contact William J. Orvis, CIAC, 510-422-8193 or send E-mail to ciac@llnl.gov.

CIAC Computer Security Information Servers

The following article is an overview of how to access CIAC's information servers and how to download information from them. Complete details for accessing these systems are available in the document: *The FELICIA Bulletin Board System and the IRBIS Anonymous FTP Server; Computer Security Information Sources for the DOE Community,* CIAC-2302, Computer Incident Advisory Capability, Lawrence Livermore National Laboratory, Livermore, CA, (1993). Contact CIAC at 510-422-8193 for a copy.

CIAC operates two file server systems for the DOE community: FELICIA, a Bulletin Board System (BBS) and IRBIS, an anonymous File Transfer Protocol (FTP) server. FELICIA is a BBS which is accessible via telephone using a modem. IRBIS is accessible via the Internet. Both of these file servers contain all of the publicly available CIAC, CERT, NIST, and DDN bulletins, virus descriptions, the virus-l moderated virus bulletin board, copies of public domain and shareware virus detection/protection software, and copies of useful public domain and shareware utility programs.

Accessing FELICIA

FELICIA is a BBS accessed via analog telephone line, a modem, and a terminal or computer running a terminal emulator program. Set your modem transmission protocol to 8 bit, no parity, one stop bit. The access numbers are:

510-423-4753 - 2400 baud or slower
510-423-3331 - 9600 baud V.32 or slower

The first time you call in, you will have to register your name and address. To download or read files, switch to the file section and follow the directions. Most of the popular downloading protocols are available, including XMODEM, YMODEM, SEALink, and Kermit.

Accessing IRBIS

IRBIS is an anonymous FTP server on the Internet, so you must have Internet access to use it. (Note: irbis.llnl.gov will change to ciac.llnl.gov in the future.) Use FTP to connect to irbis.llnl.gov (128.115.19.60). Use "anonymous" as your user name and your E-mail address as your password.

Stored in the first level directory, the file 0-index.txt is a document explaining the directory structure for downloadable files. All the computer security related files and documents are in subdirectories of the directory /pub/ciac and the file, 0-index.txt, in each subdirectory lists the other files in that directory, briefly describing their contents. The file news.txt in the /pub/ciac directory contains a list of the new files placed in the archive. Use the *get* [for single files] and *mget* [for multiple files] commands to download one or more files to your own machine.

Scanning Downloaded Software

With any software you obtain, you should exercise caution and scan individual software packages before using the software for the first time. Unless otherwise indicated, all software on FELICIA and IRBIS has been scanned for known viruses, but it is advisable to scan all downloaded software using the most recent version of a virus scanning tool. Be sure to scan archived applications after they have been extracted from the .ZIP, .ARC, or SIT archive, as most scanning software cannot detect a virus within an archived application.

Downloading Considerations

If you are downloading to a Macintosh, be sure to use the text version of the downloading protocol (e.g., Text-XMODEM, Text-YMODEM, etc. for downloads from FELICIA or ASCII mode from IRBIS) at your Macintosh when downloading pure text files or unformatted documents. The Text version of the downloading protocol corrects for the difference in the end of line characters used on the PC and Macintosh systems (the PC expects a CR-LF at the end of a line while the Macintosh expects a CR only). When downloading a binary Macintosh file such as a program file or a formatted document, be sure to set the MacBinary form of the protocol (e.g., MacBinary-XMODEM for downloads from FELICIA and Binary mode on IRBIS) on your Macintosh. If you forget to do this, you can convert later using the Apple File Exchange utility included with the Macintosh system.

Downloadable PC-DOS/MS-DOS files are either text files (.TXT), zip or arc archives (.ZIP or .ARC), self-extracting archives (.EXE) or executables (.COM or .EXE). Text files and executables can be downloaded directly and used. Be sure to use a binary downloading capability (e.g., XMODEM) for the executable files and archives. Files in ZIP archives must be extracted after downloading with PKUNZIP before they can be used. Macintosh files in SIT archives must be extracted with Stuffit before they can be used.

Macintosh files in .CPT archives must be extracted with Compactor or Extractor. SEA files on the Macintosh are self extracting archives and need no archiving program. Archiving utilities for both PC and Macintosh files are available in their respective file sections.

To obtain further information, contact William J. Orvis, CIAC, 510-422-8193 or send E-mail to ciac@llnl.gov.

OpenVMS Security Update Patch Kits

Digital Equipment Corporation has developed OpenVMS VAX and Alpha AXP patch kits for their software warranty and software contract maintenance customers. The kit for OpenVMS VAX versions 5.4-3, 5.5, 5.5-1, 5.5-2, 5.5-2H4, 5.5-2HF, and 6.0 is being tested. The kit for OpenVMS AXP versions 1.5 and 1.5-1H1 has been shipped. These kits collect a large number of patches presently available from Digital. The kits make it easy to install this collection of remedial fixes, helping those running older versions. A few of the patches provide enhanced security, hence the designation "security kit." Future releases of OpenVMS will incorporate these patches.

To obtain further information, contact Allan L. Van Lehn, CIAC, 510-422-8193 or send E-mail to ciac@llnl.gov.

CIAC Bulletins Issued in FY 93 (D-series) & FY 94 (E-series)

CIAC issues two categories of computer security announcements: the information bulletin and the advisory notice. Information bulletins describe security vulnerabilities and recommended countermeasures. Advisory notices are more imperative, urging prompt action to close vulnerabilities, either potentially or actively exploited. Advisory notices are delivered as quickly as possible via FAX, E-mail, and postal service.

D-01 Bull.	Novell NetWare Access Rights Vulnerability Any Novell NetWare 3.x, NetWare 2.x, and NetWare for Unix user, equipped with a special program, can gain the access rights assignable by any other user currently attached to the server.	October 14, 1992, 0900 PDT
D-02 Adv.	*Restricted Distribution*	October 23, 1992, 1500 PST
D-03 Bull.	Patch Available for VAX/VMS MONITOR Vulnerability Announced the availability of a kit to fix problems with VMS Versions 5.0 through 5.4-2.	October 30, 1992, 0800 PST
D-04 Bull.	18 New and Upgraded Security Patches Available For SunOS Announced security patches for SunOS versions 4.1.3, 4.1.2, 4.1.1, 4.1, 4.0.3 and Solaris 2.0 FCS (which contains SunOS 5.0).	November 11, 1992, 1200 PST
D-05 Bull.	Revised Hewlett-Packard NIS ypbind Vulnerability A revised CERT/cc ADVISORY concerns a vulnerability in the NIS ypbind module for the Hewlett-Packard (HP) series 300, 700, and 800 computers running the HP/UX Operating System.	January 22, 1993, 1400 PST

D-06 Bull.	Failure to Disable User Accounts for VMS 5.3 to 5.5-2 Local login failures to VAXstations via DECwindows or Motif for VMS versions 5.3 through Open VMS 5.5-2 will not cause an account to be DISUSERed even though sysgen parameter LGI_BRK_DISUSER is set to 1.	February 12, 1993, 1400 PST
D-07 Bull.	*Restricted Distribution*	February 23, 1993, 1700 PST
D-08 Adv.	Vulnerability in VMS V5 and Derivative Operating Systems Patch [#1084] is available for systems running VMS V5.0 through OpenVMS V5.5-2 and OpenVMS AXP V1.0 (including all SEVMS V5.1 through V5.5-2). A malicious program simplified obtaining all system privileges by authorized, unprivileged users.	February 23, 1993, 1200 PST
D-09 Bull.	OpenVMS Security Patch #1084 Problems Systems with security patch #1084 installed will not boot after performing certain system upgrades [workaround or revised patch available].	March 2, 1993, 1400 PST
D-10 Bull.	November 17 Virus on MS DOS Computers The November 17 virus [aliases: NOV 17, 855] is a MS DOS file infector which will overwrite the hard disk on November 17 of any year. Infected files grow by 768, 800, 855, or 880 bytes.	March 9, 1993, 1000 PST
D-11 Bull.	Sun Security Patches and Software Updates New patches for SunOS 4.0.3, Solaris 2.0 , 2.1 or later and new release of DECnet Interface (DNI) and PC-NFS software packages reported.	March 19, 1993, 1400 PST
D-12 Bull. D-12a Bull.	*Restricted Distribution*	April 02, 1993, 1000 PST
D-13 Adv.	wuarchive FTP Daemon Vulnerability Disable daemon, then patch or install new version of Washington University's wuarchive FTP server dated April 8 or later.	April 9, 1993, 1000 PDT
D-14 Bull.	*Restricted Distribution*	May 3, 1993, 1400 PDT
D-15 Bull.	Vulnerability in Cisco Routers used as Firewalls Under certain circumstances Cisco routers, running software releases 8.2, 8.3, 9.0, 9.1, and 9.17 using the “no IP source-route” command, will pass IP source routed packets that should be denied.	May 12, 1993, 1500 PDT
D-16 Adv.	Vulnerability in SunOS expreserve utility A patch is available for the expreserve utility in SunOS versions 4.1, 4.1.1, 4.1.2, 4.1.3, 5.0, 5.1, and 5.2 to prevent any file on the system from being overwritten [can be used to obtain root access to the system].	June 11, 1993, 0001 PDT
D-17 Bull.	*Restricted Distribution*	June 17, 1993, 1500 PDT
D-18 Bull.	Solaris 2.x expreserve patches available Expreserve patches are now available for Solaris 2.0, 2.1, and 2.2 (SunOS 5.0, 5.1, and 5.2).	July 1, 1993, 0900 PDT
D-19 Bull.	Attacks on Anonymous FTP Servers Recommendations are provided to protect against attacks on improperly configured anonymous FTP servers.	July 15, 1993, 1100 PDT
D-20 Bull.	Summary of SunOS Security Patches All security related patches currently available from Sun Microsystems.	August 6, 1993, 1200 PDT
D-21 Bull.	Novell NetWare LOGIN.EXE Security Patch Novell NetWare 4.x's LOGIN.EXE program allows inadvertent compromise of a user's name and password.	September 7, 1993, 1140 PDT
D-22 Bull.	Satan Bug Virus on MS-DOS Computers The Satan Bug virus is a new, encrypted, polymorphic virus that infects all .COM, .EXE, .SYS, and .OVL files on MS-DOS/PC-DOS computers.	September 4, 1993, 1000 PDT
D-23 Bull.	*Restricted Distribution*	September 4, 1993, 1000 PST

D-24 Bull.	SCO Home Directory Vulnerability A workaround is given for various SCO Operating Systems that permit unauthorized access to the “dos” and “asg” accounts.	September 17, 1993, 1115 PDT
D-25 Adv.	Automated Network Intrusion Software ISS or Internet Security Scanner, which does automated scanning of networked computers for security vulnerabilities, was recently made publicly available on the Internet.	September 30, 1993, 1100 PDT
D-26 Bull.	*Restricted Distribution*	September 30, 1993, 1111 PDT
E-01 Adv.	Vulnerabilities in Sun sendmail, tar, and audio The /usr/lib/sendmail utility under SunOS 4.1.x and SunOS 5.x permits unauthorized access to some system files by remote users. Archive files created with the /bin/tar utility under SunOS 5.x contain extraneous system configuration and user information from the /etc/passwd and /etc/group files should the archive files be distributed. Microphones attached to Sun workstations may be used to eavesdrop on conversations near the computer.	October 21, 1993, 1130 PDT
E-02 Bull.	Vulnerabilities in SGI IRIX Default Configuration SGI IRIX systems configured with operating system defaults and by the auto-installation procedure are vulnerable to attack.	October 25, 1993, 1330 PDT
E-03 Adv.	UNIX sendmail Vulnerabilities Details of these vulnerabilities have been openly discussed in several electronic forums, including the Firewalls mailing list and the USENET newsgroup comp.security.unix. In addition, at least one automated tool designed to exploit these vulnerabilities has been widely distributed.	November 4, 1993, 2300 PST
E-04 Bull.	xterm Logfile Vulnerability Local users may use the version 5 and earlier X11 xterm logfile facility, if installed with setuid or setgid, to create or modify files on the system. This can enable unauthorized access, including root access.	November 11, 1993, 2130 PST
E-05 Bull.	SunOS/Solbourne loadmodule and modload Vulnerability Local users may use the utilities $OPENWINHOME/bin/loadmodule and /usr/etc/modload to execute commands as root. This vulnerability only affects systems with OpenWindows 3.0 installed under SunOS 4.1.x on sun4 and Solbourne architectures.	December 15, 1993, 1200 PST
E-06 Bull.	Solaris System Startup Vulnerability A person with physical access to a workstation with eeprom(1m) security enabled can force a startup failure in fsck(8) and gain root privilege without suppllying the eeprom or root password.	December 17, 1993, 1500 PST
E-07 Bull.	UNIX sendmail Vulnerabilities Update Gives status of vendor security patches to correct vulnerabilities in the UNIX sendmail utility (see CIAC Advisory E-03). Workarounds given in E-03 may be safely used even after vendor patches have been installed.	January 7, 1994, 0900 PST
E-08 Bull.	*Restricted Distribution*	January 25, 1994, 1530 PST

To obtain further information, contact Allan L. Van Lehn, CIAC, 510-422-8193 or send E-mail to ciac@llnl.gov.

CIAC Information Technology Security Workshops

CIAC presents comprehensive, practical information technology security training and awareness workshops for technical staff and managers. These workshops enable participants to improve the security of their information technology resources. Drawing on knowledge of today’s vulnerabilities and countermeasures, we show how to prevent and respond to computer and network incidents, and leverage the DOE’s information technology security expertise for your site's greatest benefit. We tailor the workshops for your location, building it from the following self-contained modules:

Incident prevention and response
The changing nature of threats
Legal issues
Risk assessment
Electronic resources for security related information
How CIAC helps
Management policy, procedures, and programs
Managing unclassified computer security
Firewalls

CIAC bases its workshops on the latest, real world events. The workshops actively involve the participants, showing them how to protect and defend their essential resources. We actively encourage each participant to bring their concerns, challenges, and problems for group interaction and resolution. The workshops are a forum for finding solutions and an informal environment for networking with other security professionals. Upon completing the workshops, the successful participant will understand the issues and know where to find the resources necessary to prevent and effectively respond to computer and network security incidents.

There is a general session followed by separate technical and management sessions. Depending on site needs and requirements, workshops run from one to two and one-half days. There is currently no cost to DOE sites.

To request scheduling for your location or to obtain further information, contact Richard A. Feingold, CIAC, 510-422-8193 or send E-mail to ciac@llnl.gov.

CIAC Publications

A recent CIAC publication, the U.S. DOE Fingertip Guide to Incident Handling, is available from your DOE site's computer security officer (CPPM and/or CSSM).

CIAC is preparing publications on a variety of computer security related topics. Many of these will be updated as needed to keep the information current. The publications will be available in electronic form via CIAC's servers or in printed form for those who do not have Internet or telephone-modem access. Instruction on accessing these servers is provided in the article: *CIAC Computer Security Information Servers*, above. We welcome suggestions for topics that you feel would be valuable.

The publications planned for a March 1994 release are:

CIAC #	TITLE
2300	Abstracts of the CIAC-2300 Series Documents
2301	Computer Virus Information Update
2302	The FELICIA Bulletin Board System and the IRBIS Anonymous FTP Server
2303	The Console Password Feature for DEC Workstations

To obtain further information, contact Allan L. Van Lehn, CIAC, 510-422-8193 or send E-mail to ciac@llnl.gov.

End of CIAC Notes Number 01 94_01_31