

CERT Advisories

From 1988 through 2004, CERT Advisories provided system administrators and users with technical advice in response to security incidents and vulnerabilities. This collection is also available as a series of PDF digests from the [SEI Resource Library](#).

Beginning in early 2004, CERT Advisories were superseded by [US-CERT](#) (now part of [CISA](#)) [National Cyber Awareness System \(NCAS\) Alerts](#).

List of all CERT® Advisories 1988-2004

- CERT Advisory CA-1988-01 ftpd Vulnerability
- CERT Advisory CA-1989-01 Passwd hole
- CERT Advisory CA-1989-02 Sun Restore Hole
- CERT Advisory CA-1989-03 Telnet Breakin Warning
- CERT Advisory CA-1989-04 WANK Worm On SPAN Network
- CERT Advisory CA-1989-05 DEC/Ultrix 3.0 Systems
- CERT Advisory CA-1989-06 DEC/Ultrix 3.0 Systems
- CERT Advisory CA-1989-07 Sun RCP vulnerability
- CERT Advisory CA-1990-01 Sun Sendmail Vulnerability
- CERT Advisory CA-1990-02 Internet Intruder Warning
- CERT Advisory CA-1990-03 Unisys U5000 /etc/passwd problem
- CERT Advisory CA-1990-04 Apollo Domain/OS suid_exec Problem
- CERT Advisory CA-1990-05 SunView selection_svc vulnerability
- CERT Advisory CA-1990-06 NeXT's System Software
- CERT Advisory CA-1990-07 VMS ANALYZE/PROCESS_DUMP
- CERT Advisory CA-1990-08 IRIX 3.3 and 3.31 /usr/sbin/Mail
- CERT Advisory CA-1990-09 VAX/VMS Break-ins
- CERT Advisory CA-1990-10 Rumor of Alleged Attack
- CERT Advisory CA-1990-11 Security probes from Italy
- CERT Advisory CA-1990-12 SunOS TIOCCONS Vulnerability
- CERT Advisory CA-1991-01a REVISED SunOS /bin/mail Vulnerability
- CERT Advisory CA-1991-02 SunOS in.telnetd Vulnerability
- CERT Advisory CA-1991-03 Unauthorized Password Change Requests Via Mail Messages
- CERT Advisory CA-1991-04 Social Engineering
- CERT Advisory CA-1991-05 DEC Ultrix Vulnerability
- CERT Advisory CA-1991-06 NeXT rexd, /private/etc, Username me Vulnerabilities
- CERT Advisory CA-1991-07 SunOS Source Tape Installation Vulnerability
- CERT Advisory CA-1991-08 AT&T System V Release 4 /bin/login Vulnerability
- CERT Advisory CA-1991-09 Patch for SunOS /usr/etc/rpc.mountd
- CERT Advisory CA-1991-10 REVISION NOTICE: New Patch for SunOS /usr/lib/lpd
- CERT Advisory CA-1991-11 ULTRIX LAT/Telnet Gateway Vulnerability
- CERT Advisory CA-1991-12 Trusted Hosts Configuration Vulnerability
- CERT Advisory CA-1991-13 DEC ULTRIX /usr/bin/mail Vulnerability
- CERT Advisory CA-1991-14 SGI IRIX /usr/sbin/fmt Vulnerability
- CERT Advisory CA-1991-15 Mac/PC NCSA Telnet Vulnerability
- CERT Advisory CA-1991-16 SunOS SPARC Integer Division Vulnerability
- CERT Advisory CA-1991-17 DECnet-Internet Gateway Vulnerability
- CERT Advisory CA-1991-18 Active Internet tftp Attacks
- CERT Advisory CA-1991-19 AIX TFTP Daemon Vulnerability
- CERT Advisory CA-1991-20 /usr/ucb/rdist Vulnerability
- CERT Advisory CA-1991-21 NFS Jumbo Patch, SunOS 4.1
- CERT Advisory CA-1991-22 SunOS OpenWindows V3.0 Patch
- CERT Advisory CA-1991-23 Hewlett Packard/Apollo Domain/OS crp Vulnerability
- CERT Advisory CA-1992-01 NeXTstep Configuration Vulnerability
- CERT Advisory CA-1992-02 Michelangelo PC Virus Warning
- CERT Advisory CA-1992-03 Internet Intruder Activity
- CERT Advisory CA-1992-04 AT&T /usr/etc/rexecd Vulnerability
- CERT Advisory CA-1992-05 AIX REXD Daemon Vulnerability
- CERT Advisory CA-1992-06 AIX uucp Vulnerability
- CERT Advisory CA-1992-07 AIX /bin/passwd Vulnerability
- CERT Advisory CA-1992-08 Silicon Graphics Computer Systems IRIX lp Vulnerability
- CERT Advisory CA-1992-09 AIX Anonymous FTP Vulnerability
- CERT Advisory CA-1992-10 AIX crontab Vulnerability
- CERT Advisory CA-1992-11 SunOS Environment Variables and setuid/setgid Vulnerability
- CERT Advisory CA-1992-12 Revised Patch for SunOS /usr/etc/rpc.mountd Vulnerability
- CERT Advisory CA-1992-13 SunOS NIS Vulnerability
- CERT Advisory CA-1992-14 Altered System Binaries Incident
- CERT Advisory CA-1992-15 Multiple SunOS Vulnerabilities Patched
- CERT Advisory CA-1992-17 Hewlett-Packard NIS ypbind Vulnerability
- CERT Advisory CA-1992-18 Revised VMS Monitor Vulnerability
- CERT Advisory CA-1992-18 VMS Monitor Vulnerability
- CERT Advisory CA-1992-19 Keystroke Logging Banner
- CERT Advisory CA-1992-20 Cisco Access List Vulnerability
- CERT Advisory CA-1992-21 Convex CSM: migmgr patch
- CERT Advisory CA-1993-01 Revised Hewlett-Packard NIS ypbind Vulnerability
- CERT Advisory CA-1993-02 New Patch for NeXT NetInfo _writers Vulnerabilities
- CERT Advisory CA-1993-03 SunOS File/Directory Permissions

- CERT Advisory CA-1993-04 Commodore Amiga UNIX finger Vulnerability
- CERT Advisory CA-1993-05 OpenVMS and OpenVMS AXP Vulnerability
- CERT Advisory CA-1993-06 wuarchive ftpd Vulnerability
- CERT Advisory CA-1993-07 Cisco Router Packet Handling Vulnerability
- CERT Advisory CA-1993-08 SCO /bin/passwd Vulnerability
- CERT Advisory CA-1993-09a SunOS/Solaris /usr/lib/expreserve Vulnerability
- CERT Advisory CA-1993-09 SunOS/Solaris /usr/lib/expreserve Vulnerability
- CERT Advisory CA-1993-10 Anonymous FTP Activity
- CERT Advisory CA-1993-11 UMN UNIX gopher and gopher+ Vulnerabilities
- CERT Advisory CA-1993-12 Novell LOGIN.EXE Vulnerability
- CERT Advisory CA-1993-13 SCO Home Directory Vulnerability
- CERT Advisory CA-1993-14 Internet Security Scanner (ISS)
- CERT Advisory CA-1993-15 /usr/lib/sendmail, /bin/tar, and /dev/audio Vulnerabilities
- CERT Advisory CA-1993-16a Sendmail Vulnerability - supplementary advisory containing vendor patch information
- CERT Advisory CA-1993-17 xterm Logging Vulnerability
- CERT Advisory CA-1993-18 SunOS/Solbourne loadmodule and modload Vulnerability
- CERT Advisory CA-1993-19 Solaris System Startup Vulnerability
- CERT Advisory CA-1994-01 Ongoing Network Monitoring Attacks
- CERT Advisory CA-1994-02 Revised Patch for SunOS /usr/etc/rpc.mountd Vulnerability
- CERT Advisory CA-1994-03 IBM AIX Performance Tools Vulnerabilities
- CERT Advisory CA-1994-04 SunOS /usr/ucb/rdist Vulnerability
- CERT Advisory CA-1994-05 MD5 Checksums
- CERT Advisory CA-1994-06 Writable /etc/utmp Vulnerability
- CERT Advisory CA-1994-07 wuarchive ftpd Trojan Horse
- CERT Advisory CA-1994-08 ftpd Vulnerabilities
- CERT Advisory CA-1994-09 /bin/login Vulnerability
- CERT Advisory CA-1994-10 IBM AIX bsh Vulnerability
- CERT Advisory CA-1994-11 Majordomo Vulnerabilities
- CERT Advisory CA-1994-12 Sendmail Vulnerabilities
- CERT Advisory CA-1994-13 SGI IRIX Help Vulnerability
- CERT Advisory CA-1994-14 Trojan Horse in IRC Client for UNIX
- CERT Advisory CA-1994-15 NFS Vulnerabilities
- CERT Advisory CA-1995-01 IP Spoofing Attacks and Hijacked Terminal Connections
- CERT Advisory CA-1995-02 Vulnerabilities in /bin/mail
- CERT Advisory CA-1995-03 Telnet Encryption Vulnerability
- CERT Advisory CA-1995-04 NCSA HTTP Daemon for UNIX Vulnerability
- CERT Advisory CA-1995-05 Sendmail Vulnerabilities
- CERT Advisory CA-1995-05 Sendmail Vulnerability
- CERT Advisory CA-1995-06 Security Administrator Tool for Analyzing Networks (SATAN)
- CERT Advisory CA-1995-07a SATAN Vulnerability: Password Disclosure
- CERT Advisory CA-1995-07 SATAN Vulnerability: Password Disclosure
- CERT Advisory CA-1995-08 Sendmail v.5 Vulnerability
- CERT Advisory CA-1995-09 Solaris ps Vulnerability
- CERT Advisory CA-1995-10 Ghostscript Vulnerability
- CERT Advisory CA-1995-11 Sun Sendmail -oR Vulnerability
- CERT Advisory CA-1995-12 Sun 4.1.X Loadmodule Vulnerability
- CERT Advisory CA-1995-13 Syslog Vulnerability - A Workaround for Sendmail
- CERT Advisory CA-1995-14 Telnetd Environment Vulnerability
- CERT Advisory CA-1995-15 SGI lp Vulnerability
- CERT Advisory CA-1995-16 wu-ftp Misconfiguration Vulnerability
- CERT Advisory CA-1995-17 rpc.yppupdated Vulnerability
- CERT Advisory CA-1995-18 Widespread Attacks on Internet Sites
- CERT Advisory CA-1996-01 UDP Port Denial-of-Service Attack
- CERT Advisory CA-1996-02 BIND Version 4.9.3
- CERT Advisory CA-1996-03 Vulnerability in Kerberos 4 Key Server
- CERT Advisory CA-1996-04 Corrupt Information from Network Servers
- CERT Advisory CA-1996-05 Java Implementations Can Allow Connections to an Arbitrary Host
- CERT Advisory CA-1996-06 Vulnerability in NCSA/Apache CGI example code
- CERT Advisory CA-1996-07 Weaknesses in Java Bytecode Verifier
- CERT Advisory CA-1996-08 Vulnerabilities in PCNFSD
- CERT Advisory CA-1996-09 Vulnerability in rpc.statd
- CERT Advisory CA-1996-10 NIS+ Configuration Vulnerability
- CERT Advisory CA-1996-11 Interpreters in CGI bin Directories
- CERT Advisory CA-1996-12 Vulnerability in suidperl
- CERT Advisory CA-1996-13 Vulnerability in the dip program
- CERT Advisory CA-1996-14 Vulnerability in rdist
- CERT Advisory CA-1996-15 Vulnerability in Solaris 2.5 KCMS programs
- CERT Advisory CA-1996-16 Vulnerability in Solaris admintool
- CERT Advisory CA-1996-17 Vulnerability in Solaris vold
- CERT Advisory CA-1996-18 Vulnerability in fm_fls
- CERT Advisory CA-1996-19 Vulnerability in expreserve
- CERT Advisory CA-1996-20 Sendmail Vulnerabilities
- CERT Advisory CA-1996-21 TCP SYN Flooding and IP Spoofing Attacks
- CERT Advisory CA-1996-22 Vulnerabilities in bash
- CERT Advisory CA-1996-23 Vulnerability in WorkMan
- CERT Advisory CA-1996-24 Sendmail Daemon Mode Vulnerability
- CERT Advisory CA-1996-25 Sendmail Group Permissions Vulnerability
- CERT Advisory CA-1996-26 Denial-of-Service Attack via ping
- CERT Advisory CA-1996-27 Vulnerability in HP Software Installation Programs

- CERT Advisory CA-1997-01 Multi-platform Unix FLEXlm Vulnerabilities
- CERT Advisory CA-1997-02 HP-UX newgrp Buffer Overrun Vulnerability
- CERT Advisory CA-1997-03 Vulnerability in IRIX csetup
- CERT Advisory CA-1997-04 talkd Vulnerability
- CERT Advisory CA-1997-05 MIME Conversion Buffer Overflow in Sendmail Versions 8.8.3 and 8.8.4
- CERT Advisory CA-1997-06 Vulnerability in rlogin/term
- CERT Advisory CA-1997-07 Vulnerability in the httpd nph-test-cgi script
- CERT Advisory CA-1997-08 Vulnerabilities in INN
- CERT Advisory CA-1997-09 Vulnerability in IMAP and POP
- CERT Advisory CA-1997-10 Vulnerability in Natural Language Service
- CERT Advisory CA-1997-11 Vulnerability in libXt
- CERT Advisory CA-1997-12 Vulnerability in webdist.cgi
- CERT Advisory CA-1997-13 Vulnerability in xlock
- CERT Advisory CA-1997-14 Vulnerability in metamail
- CERT Advisory CA-1997-15 Vulnerability in SGI login LOCKOUT
- CERT Advisory CA-1997-16 ftpd Signal Handling Vulnerability
- CERT Advisory CA-1997-17 Vulnerability in suidperl (sperl)
- CERT Advisory CA-1997-18 Vulnerability in the at(1) program
- CERT Advisory CA-1997-19 lpr Buffer Overrun Vulnerability
- CERT Advisory CA-1997-20 JavaScript Vulnerability
- CERT Advisory CA-1997-21 SGI Buffer Overflow Vulnerabilities
- CERT Advisory CA-1997-22 BIND - the Berkeley Internet Name Daemon
- CERT Advisory CA-1997-23 Buffer Overflow Problem in rdist
- CERT Advisory CA-1997-24 Buffer Overrun Vulnerability in Count.cgi cgi-bin Program
- CERT Advisory CA-1997-25 Sanitizing User-Supplied Data in CGI Scripts
- CERT Advisory CA-1997-26 Buffer Overrun Vulnerability in statd(1M) Program
- CERT Advisory CA-1997-27 FTP Bounce
- CERT Advisory CA-1997-28 IP Denial-of-Service Attacks
- CERT Advisory CA-1998-01 Smurf IP Denial-of-Service Attacks
- CERT Advisory CA-1998-02 Vulnerabilities in CDE
- CERT Advisory CA-1998-03 Vulnerability in ssh-agent
- CERT Advisory CA-1998-04 Microsoft Windows-based Web Servers access via long file names
- CERT Advisory CA-1998-05 Multiple Vulnerabilities in BIND
- CERT Advisory CA-1998-06 Buffer Overflow in NIS+
- CERT Advisory CA-1998-07 Vulnerability in Some Usages of PKCS#1
- CERT Advisory CA-1998-08 Buffer overflows in some POP servers
- CERT Advisory CA-1998-09 Buffer Overflow in Some Implementations of IMAP Servers
- CERT Advisory CA-1998-10 Buffer Overflow in MIME-aware Mail and News Clients
- CERT Advisory CA-1998-11 Vulnerability in ToolTalk RPC Service
- CERT Advisory CA-1998-12 Remotely Exploitable Buffer Overflow Vulnerability in mountd
- CERT Advisory CA-1998-13 Vulnerability in Certain TCP/IP Implementations
- CERT Advisory CA-1999-01 Trojan horse version of TCP Wrappers
- CERT Advisory CA-1999-02 Trojan Horses
- CERT Advisory CA-1999-03 FTP Buffer Overflows
- CERT Advisory CA-1999-04 Melissa Macro Virus
- CERT Advisory CA-1999-05 Vulnerability in statd exposes vulnerability in automountd
- CERT Advisory CA-1999-06 ExploreZip Trojan Horse Program
- CERT Advisory CA-1999-07 IIS Buffer Overflow
- CERT Advisory CA-1999-08 Buffer Overflow Vulnerability in Calendar Manager Service Daemon, rpc.cmsd
- CERT Advisory CA-1999-09 Array Services deFA-19ult configuration
- CERT Advisory CA-1999-10 Insecure Default Configuration on RaQ2 Servers
- CERT Advisory CA-1999-11 Four Vulnerabilities in the Common Desktop Environment
- CERT Advisory CA-1999-12 Buffer Overflow in amd
- CERT Advisory CA-1999-13 Multiple Vulnerabilities in WU-FTP
- CERT Advisory CA-1999-14 Multiple Vulnerabilities in BIND
- CERT Advisory CA-1999-15 Buffer Overflows in SSH daemon and RSAREF2 Library
- CERT Advisory CA-1999-16 Buffer Overflow in Sun Solstice AdminSuite Daemon sadmind
- CERT Advisory CA-1999-17 Denial-of-Service Tools
- CERT Advisory CA-2000-01 Denial-of-Service Developments
- CERT Advisory CA-2000-02 Malicious HTML Tags Embedded in Client Web Requests
- CERT Advisory CA-2000-03 Continuing Compromises of DNS servers
- CERT Advisory CA-2000-04 Love Letter Worm
- CERT Advisory CA-2000-05 Netscape Navigator Improperly Validates SSL Sessions
- CERT Advisory CA-2000-06 Multiple Buffer Overflows in Kerberos Authenticated Services
- CERT Advisory CA-2000-07 Microsoft Office 2000 UA ActiveX Control Incorrectly Marked "Safe for Scripting"
- CERT Advisory CA-2000-08 Inconsistent Warning Messages in Netscape Navigator
- CERT Advisory CA-2000-09 Flaw in PGP 5.0 Key Generation
- CERT Advisory CA-2000-10 Inconsistent Warning Messages in Internet Explorer
- CERT Advisory CA-2000-11 MIT Kerberos Vulnerable to Denial-of-Service Attacks
- CERT Advisory CA-2000-12 HHCtrl ActiveX Control Allows Local Files to be Executed
- CERT Advisory CA-2000-13 Two Input Validation Problems In FTPD
- CERT Advisory CA-2000-14 Microsoft Outlook and Outlook Express Cache Bypass Vulnerability
- CERT Advisory CA-2000-15 Netscape Allows Java Applets to Read Protected Resources
- CERT Advisory CA-2000-16 Microsoft 'IE Script'/Access/OBJECT Tag Vulnerability
- CERT Advisory CA-2000-17 Input Validation Problem in rpc.statd
- CERT Advisory CA-2000-18 PGP May Encrypt Data With Unauthorized ADKs
- CERT Advisory CA-2000-19 Revocation of Sun Microsystems Browser Certificates
- CERT Advisory CA-2000-20 Multiple Denial-of-Service Problems in ISC BIND
- CERT Advisory CA-2000-21 Denial-of-Service Vulnerabilities in TCP/IP Stacks

- CERT Advisory CA-2000-22 Input Validation Problems in LPRng
- CERT Advisory CA-2001-01 Interbase Server Contains Compiled-in Back Door Account
- CERT Advisory CA-2001-02 Multiple Vulnerabilities in BIND
- CERT Advisory CA-2001-03 VBS/OnTheFly (Anna Kournikova) Malicious Code
- CERT Advisory CA-2001-04 Unauthentic "Microsoft Corporation" Certificates
- CERT Advisory CA-2001-05 Exploitation of snmpXdmid
- CERT Advisory CA-2001-06 Automatic Execution of Embedded MIME Types
- CERT Advisory CA-2001-07 File Globbing Vulnerabilities in Various FTP Servers
- CERT Advisory CA-2001-08 Multiple Vulnerabilities in Alcatel ADSL Modems
- CERT Advisory CA-2001-09 Statistical Weaknesses in TCP/IP Initial Sequence Numbers
- CERT Advisory CA-2001-10 Buffer Overflow Vulnerability in Microsoft IIS 5.0
- CERT Advisory CA-2001-11 sadmind/IIS Worm
- CERT Advisory CA-2001-12 Superfluous Decoding Vulnerability in IIS
- CERT Advisory CA-2001-13 Buffer Overflow In IIS Indexing Service DLL
- CERT Advisory CA-2001-14 Cisco IOS HTTP Server Authentication Vulnerability
- CERT Advisory CA-2001-15 Buffer Overflow In Sun Solaris in.lpd Print Daemon
- CERT Advisory CA-2001-16 Oracle 8i contains buffer overflow in TNS listener
- CERT Advisory CA-2001-17 Check Point RDP Bypass Vulnerability
- CERT Advisory CA-2001-18 Multiple Vulnerabilities in Several Implementations of the Lightweight Directory Access Protocol (LDAP)
- CERT Advisory CA-2001-19 "Code Red" Worm Exploiting Buffer Overflow In IIS Indexing Service DLL
- CERT Advisory CA-2001-20 Continuing Threats to Home Users
- CERT Advisory CA-2001-21 Buffer Overflow in telnetd
- CERT Advisory CA-2001-22 W32/Sircam Malicious Code
- CERT Advisory CA-2001-23 Continued Threat of the "Code Red" Worm
- CERT Advisory CA-2001-24 Vulnerability in OpenView and NetView
- CERT Advisory CA-2001-25 Buffer Overflow in Gauntlet Firewall allows intruders to execute arbitrary code
- CERT Advisory CA-2001-26 Nimda Worm
- CERT Advisory CA-2001-27 Format String Vulnerability in CDE ToolTalk
- CERT Advisory CA-2001-28 Automatic Execution of Macros
- CERT Advisory CA-2001-29 Oracle9iAS Web Cache vulnerable to buffer overflow
- CERT Advisory CA-2001-30 Multiple Vulnerabilities in lpd
- CERT Advisory CA-2001-31 Buffer Overflow in CDE Subprocess Control Service
- CERT Advisory CA-2001-32 HP-UX Line Printer Daemon Vulnerable to Directory Traversal
- CERT Advisory CA-2001-33 Multiple Vulnerabilities in WU-FTPd
- CERT Advisory CA-2001-34 Buffer Overflow in System V Derived Login
- CERT Advisory CA-2001-35 Recent Activity Against Secure Shell Daemons
- CERT Advisory CA-2001-36 Microsoft Internet Explorer Does Not Respect Content-Disposition and Content-Type MIME Headers
- CERT Advisory CA-2001-37 Buffer Overflow in UPnP Service On Microsoft Windows
- CERT Advisory CA-2002-01 Exploitation of Vulnerability in CDE Subprocess Control Service
- CERT Advisory CA-2002-02 Buffer Overflow in AOL ICQ
- CERT Advisory CA-2002-03 Multiple Vulnerabilities in Many Implementations of the Simple Network Management Protocol (SNMP)
- CERT Advisory CA-2002-04 Buffer Overflow in Microsoft Internet Explorer
- CERT Advisory CA-2002-05 Multiple Vulnerabilities in PHP fileupload
- CERT Advisory CA-2002-06 Vulnerabilities in Various Implementations of the RADIUS Protocol
- CERT Advisory CA-2002-07 Double Free Bug in zlib Compression Library
- CERT Advisory CA-2002-08 Multiple Vulnerabilities in Oracle Servers
- CERT Advisory CA-2002-09 Multiple Vulnerabilities in Microsoft IIS
- CERT Advisory CA-2002-10 Format String Vulnerability in rpc.rwalld
- CERT Advisory CA-2002-11 Heap Overflow in Cachefs Daemon (cachefs)
- CERT Advisory CA-2002-12 Format String Vulnerability in ISC DHCPD
- CERT Advisory CA-2002-13 Buffer Overflow in Microsoft's MSN Chat ActiveX Control
- CERT Advisory CA-2002-14 Buffer overflow in Macromedia JRun
- CERT Advisory CA-2002-15 Denial-of-Service Vulnerability in ISC BIND 9
- CERT Advisory CA-2002-16 Multiple Vulnerabilities in Yahoo! Messenger
- CERT Advisory CA-2002-17 Apache Web Server Chunk Handling Vulnerability
- CERT Advisory CA-2002-18 OpenSSH Vulnerabilities in Challenge Response Handling
- CERT Advisory CA-2002-19 Buffer Overflows in Multiple DNS Resolver Libraries
- CERT Advisory CA-2002-20 Multiple Vulnerabilities in CDE ToolTalk
- CERT Advisory CA-2002-21 Vulnerability in PHP
- CERT Advisory CA-2002-22 Multiple Vulnerabilities in Microsoft SQL Server
- CERT Advisory CA-2002-23 Multiple Vulnerabilities In OpenSSL
- CERT Advisory CA-2002-24 Trojan Horse OpenSSH Distribution
- CERT Advisory CA-2002-25 Integer Overflow In XDR Library
- CERT Advisory CA-2002-26 Buffer Overflow in CDE ToolTalk
- CERT Advisory CA-2002-27 Apache/mod_ssl Worm
- CERT Advisory CA-2002-28 Trojan Horse Sendmail Distribution
- CERT Advisory CA-2002-29 Buffer Overflow in Kerberos Administration Daemon
- CERT Advisory CA-2002-30 Trojan Horse tcpdump and libpcap Distributions
- CERT Advisory CA-2002-31 Multiple Vulnerabilities in BIND
- CERT Advisory CA-2002-32 Backdoor in Alcatel OmniSwitch AOS
- CERT Advisory CA-2002-33 Heap Overflow Vulnerability in Microsoft Data Access Components (MDAC)
- CERT Advisory CA-2002-34 Buffer Overflow in Solaris X Window Font Service
- CERT Advisory CA-2002-35 Vulnerability in RaQ Server Appliances
- CERT Advisory CA-2002-36 Multiple Vulnerabilities in SSH Implementations
- CERT Advisory CA-2002-37 Buffer Overflow in Microsoft Windows Shell
- CERT Advisory CA-2003-01 Buffer Overflows in ISC DHCPD Minires Library
- CERT Advisory CA-2003-02 Double-Free Bug in CVS Server
- CERT Advisory CA-2003-03 Buffer Overflow in Windows Locator Service
- CERT Advisory CA-2003-04 MS-SQL Server Worm

- CERT Advisory CA-2003-05 Multiple Vulnerabilities in Oracle Servers
- CERT Advisory CA-2003-06 Multiple vulnerabilities in implementations of the Session Initiation Protocol (SIP)
- CERT Advisory CA-2003-07 Remote Buffer Overflow in Sendmail
- CERT Advisory CA-2003-08 Increased Activity Targeting Windows Shares
- CERT Advisory CA-2003-09 Buffer Overflow in Core Microsoft Windows DLL
- CERT Advisory CA-2003-10 Integer overflow in Sun RPC XDR library routines
- CERT Advisory CA-2003-11 Multiple Vulnerabilities in Lotus Notes and Domino
- CERT Advisory CA-2003-12 Buffer Overflow in Sendmail
- CERT Advisory CA-2003-13 Multiple Vulnerabilities in Snort Preprocessors
- CERT Advisory CA-2003-14 Buffer Overflow in Microsoft Windows HTML Conversion Library
- CERT Advisory CA-2003-15 Cisco IOS Interface Blocked by IPv4 Packet
- CERT Advisory CA-2003-16 Buffer Overflow in Microsoft RPC
- CERT Advisory CA-2003-17 Exploit available for for the Cisco IOS Interface Blocked Vulnerabilities
- CERT Advisory CA-2003-18 Integer Overflows in Microsoft Windows DirectX MIDI Library
- CERT Advisory CA-2003-19 Exploitation of Vulnerabilities in Microsoft RPC Interface
- CERT Advisory CA-2003-20 W32/Blaster worm
- CERT Advisory CA-2003-21 GNU Project FTP Server Compromise
- CERT Advisory CA-2003-22 Multiple Vulnerabilities in Microsoft Internet Explorer
- CERT Advisory CA-2003-23 RPCSS Vulnerabilities in Microsoft Windows
- CERT Advisory CA-2003-24 Buffer Management Vulnerability in OpenSSH
- CERT Advisory CA-2003-25 Buffer Overflow in Sendmail
- CERT Advisory CA-2003-26 Multiple Vulnerabilities in SSL/TLS Implementations
- CERT Advisory CA-2003-27 Multiple Vulnerabilities in Microsoft Windows and Exchange
- CERT Advisory CA-2003-28 Buffer Overflow in Windows Workstation Service
- CERT Advisory CA-2004-01 Multiple H.323 Message Vulnerabilities
- CERT Advisory CA-2004-02 Email-borne Viruses