

# SAFER

SECURITY ALERT FOR ENTERPRISE RESOURCES

**Volume 4 Issue 10**

**October 2001**

*A monthly publication of eGlobal Technology. Copyright © 2001 All rights reserved.  
For further information or comments please contact [security@safermag.com](mailto:security@safermag.com)*

eGlobal Technology produces this newsletter to aid and assist security-concerned executives and IT professionals. eGlobal Technology's comments are opinions only. No action can be taken against eGlobal Technology for following comments or for any consequence of action emanating from the reading of this newsletter.

SAFER subscriptions can be made at <http://www.safermag.com>

# CONTENTS

<b>CONTENTS</b> .....	<b>2</b>
<b>EXECUTIVE NEWS</b> .....	<b>5</b>
GENERAL NEWS .....	5
EUROPE – MIDDLE-EAST .....	6
UNITED STATES - CANADA .....	6
ASIA - PACIFIC .....	7
<b>SECURITY ALERTS</b> .....	<b>8</b>
NAI PGP KEYSERVER WEB ADMINISTRATION INTERFACE AUTHENTICATION BYPASSING VULNERABILITY.....	8
CHARLES CLARK METEOR FTP DIRECTORY TRAVERSAL VULNERABILITY .....	8
COM2001 ALEXIS SERVER WEB ACCESS PLAINTEXT PASSWORD VULNERABILITY .....	9
AMTOTE HOMEBET ACCOUNT INFORMATION BRUTE FORCE VULNERABILITY.....	9
AMTOTE HOMEBET WORLD ACCESSIBLE LOG VULNERABILITY .....	9
OPENSSSH KEY BASED SOURCE IP ACCESS CONTROL BYPASS VULNERABILITY .....	10
MICROSOFT EXCHANGE OWA SERVER RESOURCE STARVATION VULNERABILITY .....	10
REDHAT SETSERIAL INIT SCRIPT PREDICTABLE TEMPORARY FILE VULNERABILITY .....	10
CISCO PIX FIREWALL SMTP CONTENT FILTERING EVASION VULNERABILITY RE-INTRODUCTION .....	11
SLRN ARBITRARY SHELL SCRIPT EXECUTION VULNERABILITY .....	11
PHPNUKE REMOTE FILE COPY VULNERABILITY.....	11
MICHAEL BARRETTO CARDBOARD REMOTE COMMAND EXECUTION VULNERABILITY .....	12
H-SPHERE ARBITRARY FILE DISCLOSURE VULNERABILITY .....	12
INTERSHOP COMMUNICATIONS INTERSHOP ARBITRARY COMMAND EXECUTION VULNERABILITY .....	12
HYLAFAX HOSTNAME FORMAT STRING VULNERABILITY .....	13
BALTIMORE TECHNOLOGIES MAILSWEEPER SCRIPT FILTERING BYPASS VULNERABILITY .....	13
XCACHE PATH DISCLOSURE VULNERABILITY .....	13
HALF-LIFE CLIENT SIDE CONNECT BUFFER OVERFLOW VULNERABILITY .....	14
PI-SOFT SPOONFTP DIRECTORY TRAVERSAL VULNERABILITY .....	14
LOTUS DOMINO INTERNAL IP ADDRESS DISCLOSURE VULNERABILITY .....	14
IBM WEBSPHERE APPLICATION SERVER PREDICTABLE SESSION ID VULNERABILITY .....	15
JOHN E. DAVIS MOST BUFFER OVERFLOW VULNERABILITY .....	15
ZyXEL PRESTIGE 642R ROUTER WAN PORT FILTER BYPASS VULNERABILITY .....	15
ORACLE 9I APPLICATION SERVER PATH REVEALING VULNERABILITY .....	16
COMPUTER ASSOCIATES ARCSERVE CLEARTEXT ADMINISTRATIVE PASSWORD VULNERABILITY .....	16
COMPUTER ASSOCIATES ARCSERVE INSECURE DEFAULT NETWORK SHARE VULNERABILITY .....	16
WEBDISCOUNT E-SHOP REMOTE ARBITRARY COMMAND EXECUTION VULNERABILITY .....	17
MICROSOFT INDEX SERVER 2.0 FILE INFORMATION AND PATH DISCLOSURE VULNERABILITY .....	17
COUNTERPANE PASSWORD SAFE DATA BUFFER RECOVERY VULNERABILITY .....	17
CHECK POINT FIREWALL-1 GUI LOG VIEWER VULNERABILITY .....	18
RED HAT LINUX APACHE REMOTE USERNAME ENUMERATION VULNERABILITY .....	18
MICROSOFT OUTLOOK EXPRESS 6 PLAIN TEXT MESSAGE SCRIPT EXECUTION VULNERABILITY .....	18
EFTP SERVER DIRECTORY AND FILE EXISTENCE VULNERABILITY .....	19
EFTP CLEAR TEXT PASSWORD STORAGE VULNERABILITY .....	19
EFTP PASSWORD HASH RETRIEVAL VULNERABILITY.....	19
RSA BSAFE SSL-J AUTHENTICATION BYPASS VULNERABILITY.....	20
TEXTOR WEBMASTERS LIMITED LISTREC.PL INPUT VALIDATION VULNERABILITY .....	20
TREND MICRO INTERSCAN eMANAGER BUFFER OVERFLOW VULNERABILITY .....	20
SPEECHD PRIVILEGED COMMAND EXECUTION VULNERABILITY.....	21
APPLE MACINTOSH OS X FBCINDEX FILE CONTENTS DISCLOSURE VULNERABILITY .....	21
APPLE MACINTOSH OS X .DS_STORE DIRECTORY LISTING DISCLOSURE VULNERABILITY .....	21
NETOP SCHOOL ADMINISTRATION AUTHENTICATION VULNERABILITY .....	22
DIGITAL UNIX MSGCHK MH_PROFILE SYMBOLIC LINK VULNERABILITY.....	22
LEON J BREEDT PAM-PSQL REMOTE SQL QUERY MANIPULATION VULNERABILITY .....	22
JOERG WENDLAND PAM-PSQL REMOTE SQL QUERY MANIPULATION VULNERABILITY.....	23
MACOS X CLIENT APACHE DIRECTORY CONTENTS DISCLOSURE VULNERABILITY.....	23
NSS NSS_PostgreSQL REMOTE SQL QUERY MANIPULATION VULNERABILITY .....	23
JOERG WENDLAND LIBNSS-PgSQL REMOTE SQL QUERY MANIPULATION VULNERABILITY .....	24
DIGITAL UNIX MSGCHK BUFFER OVERFLOW VULNERABILITY .....	24
TAYLOR UUCP ARGUMENT HANDLING PRIVILEGE ELEVATION VULNERABILITY .....	24
CHECK POINT FIREWALL-1 GUI CLIENT LOG VIEWER SYMBOLIC LINK VULNERABILITY .....	25

SEAGLASS TECHNOLOGIES SGLMERCHANT DIRECTORY TRAVERSAL VULNERABILITY .....	25
HASSAN CONSULTING SHOPPING CART ARBITRARY COMMAND EXECUTION VULNERABILITY .....	25
CHECK POINT FIREWALL-1 POLICYNAME TEMPORARY FILE CREATION VULNERABILITY .....	26
NORTON ANTI-VIRUS FOR MICROSOFT EXCHANGE 2000 INFORMATION DISCLOSURE VULNERABILITY .....	26
PROFTPD CLIENT HOSTNAME RESOLVING VULNERABILITY .....	27
POWER UP HTML DIRECTORY TRAVERSAL ARBITRARY FILE DISCLOSURE VULNERABILITY .....	27
MERIT AAA RADIUS SERVER RLMADMIN SYMBOLIC LINK VULNERABILITY .....	27
MICROSOFT EXCHANGE OWA GLOBAL ADDRESS LIST DISCLOSURE VULNERABILITY .....	28
NETBSD SEMOP ARBITRARY CODE EXECUTION VULNERABILITY .....	28
BALTIMORE TECHNOLOGIES WEBSWEEPER RESTRICTED DIRECTORY DISCLOSURE VULNERABILITY .....	28
GNU MAILMAN EMPTY PASSWORD BLANK SALT VULNERABILITY .....	29
SHOPPLUS CART ARBITRARY COMMAND EXECUTION VULNERABILITY .....	29
MULTIPLE IDS VENDOR ENCODED IIS ATTACK DETECTION EVASION VULNERABILITY .....	30
GAUNTLET FIREWALL FOR UNIX AND WEBSHIELD CSMAP AND SMAP/SMAPD BUFFER OVERFLOW VULN. ....	30
HP-UX LOGIN BTMP LOGGING FAILURE VULNERABILITY .....	31
VIBECCHILD DIRECTORY MANAGER COMMAND EXECUTION VULNERABILITY .....	31
INFORMIX SQL SNMPDM PREDICTABLE TEMPORARY FILE CREATION VULNERABILITY .....	31
INTER7 VPOPMAIL MYSQL AUTHENTICATION DATA RECOVERY VULNERABILITY .....	32
INFORMIX SQL ONSRVAPD PREDICTABLE TEMPORARY FILE CREATION VULNERABILITY .....	32
FREEBSD RMUSER PASSWORD HASH DISCLOSURE VULNERABILITY .....	32
INFORMIX SQL TEMPORARY LOG FILE SYMBOLIC LINK VULNERABILITY .....	33
PGP INVALID KEY DISPLAY VULNERABILITY .....	33
HP-UX SWVERIFY BUFFER OVERFLOW VULNERABILITY .....	33
POP3LITE INPUT VALIDATION VULNERABILITY .....	34
<b>SECURITY ADVISORIES.....</b>	<b>35</b>
CONECTIVA ANNOUNCEMENT CLA-2001:427: MOD_AUTH_PGSQL .....	35
CALDERA SECURITY ADVISORY CSSA-2001-SCO.20: BUFFER OVERFLOW IN BSD LINE PRINTER DAEMON ....	35
MICROSOFT SECURITY BULLETIN (MS01-049) .....	35
CISCO SECURITY ADVISORY: CISCO SECURE PIX FIREWALL SMTP FILTERING VULNERABILITY .....	36
CONECTIVA ANNOUNCEMENT CLA-2001:426: SQUID .....	36
LINUX-MANDRAKE SECURITY UPDATE MDKA-2001:015: LYX .....	36
UPDATE IS AVAILABLE FROM MANDRAKE. DEBIAN SECURITY ADVISORY DSA-079-1: UUCP .....	36
HP SECURITY BULLETIN #0167: VULNERABILITY IN CU(1) .....	37
DEBIAN SECURITY ADVISORY DSA-078-1: SLRN .....	37
FREEBSD SECURITY ADVISORY SA-01:60: PROCMAIL .....	37
DEBIAN SECURITY ADVISORY DSA-077-1: SQUID .....	37
CALDERA SECURITY ADVISORY CSSA-2001-SCO.19: XLOCK BUFFER OVERFLOW .....	38
LINUX-MANDRAKE SECURITY UPDATE MDKSA-2001:078: UUCP .....	38
CALDERA SECURITY ADVISORY CSSA-2001-SCO.18: SU BUFFER OVERFLOW .....	38
SUSE SECURITY ANNOUNCEMENT SuSE-SA:2001:032: WMAKER/WINDOWMAKER .....	38
CALDERA SECURITY ADVISORY CSSA-2001-SCO.17: VI/TMP VULNERABILITY .....	38
RED HAT SECURITY ADVISORY RHSA-2001:110-05: INITSRIPT .....	39
DEBIAN SECURITY ADVISORY DSA-076-1: MOST .....	39
CALDERA SECURITY ADVISORY CSSA-2001-SCO.16: LP UTILITY COMMANDS .....	39
LINUX-MANDRAKE SECURITY UPDATE MDKSA-2001:077: APACHE .....	40
CISCO SECURITY ADVISORY: VULNERABLE SSL IMPLEMENTATION IN ICDN .....	40
LINUX-MANDRAKE SECURITY UPDATE MDKSA-2001:073-1: XLI/XLOADIMAGE .....	40
CONECTIVA ANNOUNCEMENT CLA-2001:425: UUCP .....	41
HP SECURITY BULLETIN #0145: VULNERABILITY IN ASEURE (REV.03) .....	41
SUSE SECURITY ANNOUNCEMENT SuSE-SA:2001:31: APACHE-CONTRIB .....	41
RED HAT SECURITY ADVISORY RHSA-2001:107-07: BUGZILLA .....	41
MICROSOFT SECURITY BULLETIN (MS01-048) .....	42
NETBSD SECURITY ADVISORY 2001-017: SENDMAIL(8) INCORRECT COMMAND LINE ARGUMENT CHECK .....	42
CALDERA SECURITY ADVISORY CSSA-2001-033.0: LINUX - UUCP ARGUMENT HANDLING PROBLEMS .....	42
NETBSD SECURITY ADVISORY 2001-016: UNSAFE CHDIR USAGE IN FTS(3) .....	42
RED HAT SECURITY ADVISORY RHSA-2001:109-05: XINETD .....	43
IBM MSS ADVISORY MSS-OAR-E01-2001:391.1: BUFFER OVERFLOW VULNERABILITIES IN LPD .....	43
FREEBSD SECURITY ADVISORY SA-01:57: SENDMAIL (REVISED) .....	43
RED HAT SECURITY ADVISORY RHSA-2001:106-06: SENDMAIL .....	44
NETBSD SECURITY ADVISORY 2001-015: INSUFFICIENT CHECKING OF LENGTHS PASSED TO KERNEL .....	44
MICROSOFT SECURITY BULLETIN (MS01-047) .....	44
RED HAT SECURITY ADVISORY RHSA-2001:103-04: FETCHMAIL .....	45
CONECTIVA ANNOUNCEMENT CLA-2001:421: MOD_AUTH_MYSQL .....	45

RED HAT SECURITY ADVISORY RHSA-2001:072-14: MAN .....	45
HP SECURITY BULLETIN #0166: VULNERABILITY IN LIBSECURITY (VVOS).....	45
SUSE SECURITY ANNOUNCEMENT SuSE-SA:2001:030: SCREEN.....	46
ISS ALERT: MULTIPLE VENDOR IDS UNICODE BYPASS VULNERABILITY .....	46
CONECTIVA ANNOUNCEMENT CLA-2001:420: MAILMAN .....	47
CISCO SECURITY ADVISORY: CISCO SECURE IDS SIGNATURE OBFUSCATION VULNERABILITY.....	47
CONECTIVA ANNOUNCEMENT CLA-2001:419: FETCHMAIL.....	47
FREEBSD SECURITY ADVISORY SA-01:59: RMUSER (REVISED) .....	48
SUSE SECURITY ANNOUNCEMENT SuSE-SA:2001:029: NKITB/NKITSERV/TELNETD .....	48
LINUX-MANDRAKE SECURITY UPDATE MDKSA-2001:076: XINETD .....	49
LINUX-MANDRAKE SECURITY UPDATE MDKSA-2001:075: SENDMAIL.....	49
LINUX-MANDRAKE SECURITY UPDATE MDKSA-2001:074: WINDOWMAKER.....	49
LINUX-MANDRAKE SECURITY UPDATE MDKSA-2001:073: XLI .....	49
LINUX-MANDRAKE SECURITY UPDATE MDKSA-2001:072: FETCHMAIL .....	50
<b>DENIAL-OF-SERVICE .....</b>	<b>51</b>
3COM HOMECONNECT CABLE MODEM EXTERNAL WITH USB DENIAL OF SERVICE VULNERABILITY .....	51
QPC SOFTWARE QVT/TERM FTP DENIAL OF SERVICE VULNERABILITY .....	51
COMPAQ TRUCLUSTER PORT SCAN DENIAL OF SERVICE VULNERABILITY .....	51
IBM HACMP PORT SCAN DENIAL OF SERVICE VULNERABILITY .....	52
SQUID WEB PROXY CACHE DENIAL OF SERVICE VULNERABILITY .....	52
HP-UX VVOS LIBSECURITY DENIAL OF SERVICE VULNERABILITY.....	52
EFTP BUFFER OVERFLOW CODE EXECUTION AND DENIAL OF SERVICE VULNERABILITY .....	53
MICROSOFT WINDOWS NT RPC ENDPOINT MAPPER DENIAL OF SERVICE VULNERABILITY.....	53
DLINK IP FRAGMENT DENIAL OF SERVICE VULNERABILITY .....	53
NETBSD IOCTL DENIAL OF SERVICE VULNERABILITY .....	54
MARCONI FORTHOUGHT 7.1 TELNET ADMINISTRATION DENIAL OF SERVICE VULNERABILITY .....	54
<b>UNDERGROUND TOOLS .....</b>	<b>55</b>

# EXECUTIVE NEWS

*What follows is the author's selection of rumors and noises of concern to the security community. We welcome your comments and opinions.*

---

## General News

---

- **Self-executing virus attacks IIS and Microsoft Outlook.** Experts are tracking a fast-spreading virus that propagates both by sending itself as an email attachment, and by hacking into vulnerable web servers. According to an analysis by SecurityFocus' ARIS analysis team, the W32.Nimda.A@mm worm spreads by infecting Microsoft IIS servers that are open to known software vulnerabilities: the IIS 4.0/5.0 File Permission Canonicalization Vulnerability, the IIS/PWS Escaped Characters Decoding Command Execution Vulnerability, and the IIS/PWS Extended Unicode Directory Traversal Vulnerability. Fixes for all three holes are available from Microsoft. The worm also attacks Microsoft Outlook users, arriving as an apparently blank message with an attachment called 'readme.exe'. But unlike most so-called mass mailers, Nimda can infect Outlook and Outlook Express users who know better than to open strange attachments. By exploiting a bug in older versions of Internet Explorer discovered last March, the worm is able to infect victim computers when the email is read, or even displayed in Outlook's preview pane.
- **Experts are calling it a security manager's nightmare.** For the second time in as many years, a hole has been discovered in Network Associate's Gauntlet firewall software that makes it possible for intruders to turn the security system against the very networks it was designed to protect, SecurityFocus has learned. On Tuesday, the company's PGP Security division quietly released patches for a buffer overflow vulnerability in the firewall's 'csmmap' SMTP proxy, a feature of the firewall that, ironically, is designed to act as a protective membrane between an organization's mail server application and the rest of the world. In normal operation, csmmap accepts mail connections from the Internet, and then forwards only valid traffic to the internal mail server. By adding reams of text at a particular point in the mail transaction, an attacker can overflow the memory dedicated to storing an email address. Properly crafted computer instructions appended to the text will then be executed by the machine, giving hackers a way in. The bug affects users of Gauntlet 5.0, 5.5 and 6.0 on Solaris and HP-UX, and the company's Web Shield line of appliances. The hole is the second serious security hole to be found in Gauntlet. Last year, Network Associates' integration of Mattel's Cyber Patrol filtering software into the product created another buffer overflow vulnerability that potentially gave attackers remote 'root' level access to the machine.
- **Why is it that, when four out of five IT-related crimes are committed from within an organisation,** most companies still believe that the only threat comes from faceless hackers and virus writers? External threats should be taken seriously, and protection put in place, but nobody knows your security loopholes better than your employees. Despite their common occurrence, internal security breaches go largely unreported. What company wants to publicise that sensitive information has been accessed from within? Employees understand in detail how their organisation's systems work. If someone has access to passwords they also have access to confidential information. An expert can also exploit software weaknesses to introduce viruses or gain access, or use hacking tools designed for Denial of Service, intrusion or password cracking to cause mayhem. Employees can unwittingly open a company's innermost secrets through sheer carelessness, and the most damaging viruses have spread because people open email attachments. Another problem is remote workers turning off security protection on laptops.
- **A war against terrorism raises the specter of increased security risks for information managers** — risks ranging from nuisance Web site defacements to the possibility that systems could be targeted in conjunction with a physical attack as part of an effort to maximize disruptions. Such threats existed before the Sept. 11 terrorist attacks against the U.S. But the possibility of a significant attack specifically, a combined cyber and physical assault—is being taken much more seriously since those events. What security experts and managers are less certain of is the degree of risk. Most said they believe the war against terrorism will raise the danger level, but some security managers said they were already under siege. "I think we already had a very significant threat prior to Sept. 11," said Steve Akridge, chief security officer for the Georgia Technology Authority, which manages the state's IT. "On a scale of 1 to 10, we felt that the threat was an 8. Maybe now it's a 9," said Akridge. The biggest change wrought by the terrorist attacks may be improved awareness of the importance of information security—especially contingency planning. "Even though it wasn't a computer-related attack, the mind-set now is that we are no longer immune from this type of incident," said Larry Seibel, information security director at the

Huntington National Bank in Columbus, Ohio. "The incident, without a doubt, has served to raise the level of importance of contingency planning for business and systems recovery."

- **Computer hackers come in many shades -- extortion artists, corporate saboteurs, determined teenagers and legitimate IT professionals.** But according to security experts at IBM, they have one thing in common: Every office has at least one. Seizing upon the timely topic of Internet security risks, IBM this week has launched a global advertising and public relations initiative to plug its e-business security software and consulting expertise. Business managers, concerned at the threat of attack, are fortifying their internal computer systems. Last week, a Corporation for British Industry survey revealed that two-thirds of UK businesses have been the victim of a serious computer-related incident, whether it be hacking, a virus attack or some form of cyber-fraud. It means that software firms and security consultancies may once again have a big market for their services. (2/3 had problems 5 years ago, 2/3 have problems now – statistics will never change, it seems – ed.)

---

## Europe – Middle-East

---

- **PARIS -- At any other time, a gathering of privacy mavens,** policy-makers and legal experts in Paris might make for an interesting if laidback discussion on the ethical niceties of balancing national security and personal privacy. In the aftermath of the terrorist attacks on the United States, such debates have taken on an intensity and urgency that two weeks and 3,500 miles of ocean cannot diminish. French President Jacques Chirac set the tone for delegates at the 23rd International Conference of Data Protection Commissioners, telling them to "respect freedom of thought, but don't let the Internet become the tool of the enemies of liberty and human dignity. He also called for international cooperation to stamp out cybercrime and implement a transnational system of law for dealing with abuse. "Taking into account the global dimension of the Internet, it is essential to put in place an efficient and progressive universal legal framework which clearly defines infractions and proposes procedures for penalizing them," he said.
- **At last week's IQPC Electronic Signature Summit influential delegates from blue chip and global businesses voiced their dissatisfaction** with the Government's support of Internet security. The event included speakers from the Department of Trade and Industry, the Public Key Infrastructure (PKI) Forum, tScheme, the Global Trust Authority, the Confederation of British Industry and the British Bankers Association. Security company De La Rue InterClear, organised a survey of attendees which found that 80 per cent believed the Government was not doing enough to promote e-security in this country. The survey showed network managers have become disillusioned by the Government's lack of understanding of e-security issues. Four out of five respondents believed that education was the most important activity that Government should undertake, while half said new legislation was key.

---

## United States - Canada

---

- **Justice Department proposal classifies most computer crimes as acts of terrorism.** Hackers, virus-writers and web site defacers would face life imprisonment without the possibility of parole under legislation proposed by the Bush Administration that would classify most computer crimes as acts of terrorism. The Justice Department is urging Congress to quickly approve its Anti-Terrorism Act (ATA), a twenty-five page proposal that would expand the government's legal powers to conduct electronic surveillance, access business records, and detain suspected terrorists. The proposal defines a list of "Federal terrorism offenses" that are subject to special treatment under law. The offenses include assassination of public officials, violence at international airports, some bombings and homicides, and politically motivated manslaughter or torture. Most of the terrorism offenses are violent crimes, or crimes involving chemical, biological, or nuclear weapons. But the list also includes the provisions of the Computer Fraud and Abuse Act that make it illegal to crack a computer for the purpose of obtaining anything of value, or to deliberately cause damage. Likewise, launching a malicious program that harms a system, like a virus, or making an extortionate threat to damage a computer are included in the definition of terrorism. To date no terrorists are known to have violated the Computer Fraud and Abuse Act.
- **Credit card giant prepares to crack down on insecure e-commerce sites.** Eager to dispel consumer fears over online shopping, credit card leader Visa U.S.A. announced a plan this week to accomplish by force and reason what lawless cyberpunks have failed to do through public humiliation: get web merchants to protect credit card numbers and customer data from hack attacks. Under the plan, the California-based credit card association will begin monitoring the thousands of online businesses that accept Visa transactions, to ensure compliance with the company's written security standards. Those standards are built on staples like firewall use, cryptography, and up-to-date vulnerability patching. "These are the types of security requirements

that we believe, at a minimum, anyone doing business in the Internet space should be at," says Jean Bruesewitz, Visa's vice president of advanced risk solutions. Merchants who aren't in ship shape could be hit with financial penalties. The exact shape of the monitoring has yet to be determined, but Visa plans to begin in May, 2001, and is launching a voluntary program to gently guide e-businesses into compliance before that deadline. "We aren't going to rush into the monitoring, because we want to let them go through a self-assessment process and assess their own security first," says Bruesewitz. Participating businesses will be given self-assessment tests to evaluate their own level of security.

- **When the world's most famous crypto patent turns sweet seventeen, it will be in the prime of its life.** Most of the 1,334 United States patents that will turn 17-years-old and expire on September 20th will not kick-off raucous celebration around the country. When the patent for a particular timed telephone ring silencer device becomes usable by anyone *sans* licensing fees, champagne glasses will not tilt for it. Likewise, a combined denture mold dewaxer and curing basin, a circuit for distorting an audio signal, and a process for preparing acetic acid esters will all slip into the public domain without so much as a handful of confetti taking flight in their honor. But U.S. patent number 4,405,829, "Cryptographic Communications System And Method," is another story. Named for its inventors, Rivest, Shamir, and Adleman, the RSA crypto system has become the de-facto standard for public key cryptography. RSA can be used attach tamper-proof signatures to digital documents; it can protect electronic communications on the fly without users agreeing in advance on a common key with which to lock their secrets. Since MIT patented the system in 1983, then licensed it exclusively to a company formed to exploit the patent, the RSA algorithm has aged like a fine wine on the tannin of cryptanalysis and unsuccessful attack. Mathematicians admire RSA for its elegance--the algorithm derives its security from natural limitations in factoring large prime numbers. Information security engineers like it because criminals can't crack it; cypherpunks like it because the NSA can't crack it.

---

## Asia - Pacific

---

- **There were 5,000 attempts by professional hackers to invade the Dubai Police computer network in the two hours prior to a visit by General Sheikh Mohammed bin Rashid Al Maktoum,** Crown Prince of Dubai and Minister of Defence, to the Officers Club on June 15, a senior officer has revealed. Issa Salem Al Jalaf, head of police Strategic Planning, said that by the time of Sheikh Mohammed's visit, when all car number plates had been stored in the network, hackers attempted to invade it. Al Jalaf, who is General Coordinator of Dubai e-government, said the full resources of the police and Emirates Telecommunications Corp (Etisalat) were used to foil the hackers. Al Jalaf was speaking at the Ras Al Khaimah Police Officers Club during a seminar on "The Security of Information and Computer Crimes". About eight per cent of the hackers are employed by UAE companies. Many of them planned post-graduate studies to become as professional as possible in their destructive activities, he said. Many UAE companies have lost billions of dirhams as a result of hacking. Yet the UAE does not have a law specifically banning hacking, although the Ministry of Justice is preparing one. Hackers are charged on the basis of laws dealing with comparable crimes, he said. (one has to wonder how they know what was attempt by 'professional hacker', and what was an attempt by 'hobbyist' – ed.)

# SECURITY ALERTS

*We try to inform you of vulnerabilities as soon as they become a threat to your resources, not when the vendors decide to report them.*

---

## NAI PGP Keyserver Web Administration Interface Authentication Bypassing Vulnerability

---

**Released** September 28, 2001

**Affects** Network Associates PGP Keyserver 7.0 and 7.0.1

**Reference** <http://www.securityfocus.com/cgi-bin/vulns-item.pl?section=info&id=3375>

### Problem

- A problem with the key server could make it possible for remote users to compromise the integrity of posted keys. This could lead to a potential compromise public keys, and potentially sensitive information.
- The problem is due to inadequate access control of executables included with the package. When the web administration interface is accessed by the key server administrator, the programs [http://www.example.com/keyserver/cgi-bin/console.exe?page\\_size=...](http://www.example.com/keyserver/cgi-bin/console.exe?page_size=...) and <http://www.example.com/keyserver/cgi-bin/cs.exe?action=...> are used by the infrastructure to carry out the commands of the administrator to the interface.
- However, strict authentication is not enforced on these programs. A remote user could access these programs directly, and carry out commands on the system without challenge. This could result in a denial of service situation, where the PGP Key database is removed. Worse, this could result in the placement of malicious PGP Keys, which could be exploited to gain access to sensitive email and other documents.

### SAFER

- NAI has provided a workaround at <http://www.pgp.com/support/product-advisories/keyserver.asp>.

---

## Charles Clark Meteor FTP Directory Traversal Vulnerability

---

**Released** September 28, 2001

**Affects** Charles Clark Meteor FTP 1.0

**Reference** <http://www.securityfocus.com/cgi-bin/vulns-item.pl?section=info&id=3374>

### Problem

- Authenticated users can gain read access to the directories of the host where the FTP server has been installed. Through the use of '..', '/../' or '...' sequences when submitting a 'ls' command, arbitrary directories and files could be disclosed, potentially compromising the privacy of user data and/or obtaining information which could be used to further compromise the host's security.
- If successfully exploited this vulnerability could lead to the disclosure of sensitive information assisting in further attacks against the host.

### SAFER

- Charles Clark has released a fixed version of Meteor FTP.

---

## COM2001 Alexis Server Web Access Plaintext Password Vulnerability

---

**Released** September 28, 2001

**Affects** COM2001 Alexis Server 2.0 and 2.1

**Reference** <http://www.securityfocus.com/cgi-bin/vulns-item.pl?section=info&id=3373>

### Problem

- The Web Access component in Alexis Server has a tendency to transmit information in plaintext, including authentication credentials such as username/password. Alexis Server v2.1 has the option to secure transmissions using SSL. However, as a side effect the Web Access toolbar will open a java applet which sends the information back to the server (on port 8888, by default) in plaintext. If the transmitted information is sniffed at this point then the username/password will be disclosed to the attacker.
- Alexis v2.0 does not include the option of using SSL to secure communications, so it should be considered to be extra vulnerable to this issue.
- It should be noted that Alexis Server v1.1 is not prone to this issue as it does not use the voicemail username/password for Web Access.
- Successful exploitation of this issue will allow a remote attacker to gain unauthorized access to voicemail and PBX services.

### SAFER

- Workaround: Use a firewall to block access to port 8888 of the affected host. This will affect some functionality, such as call screening, etc. The vendor is aware of this issue and will release a fix in an upcoming service pack.

---

## AmTote Homebet Account Information Brute Force Vulnerability

---

**Released** September 28, 2001

**Affects** AmTote Homebet

**Reference** <http://www.securityfocus.com/cgi-bin/vulns-item.pl?section=info&id=3371>

### Problem

- A vulnerability exists in Homebet which could enable a non-registered user to confirm the validity of possible legitimate users and their PIN numbers.
- If an invalid account number is supplied by a remote client, a specific error page will be returned to the user. A different error page is generated if the account number is valid but the PIN is incorrect. These contrasting error pages will permit an attacker to easily determine valid account numbers, making more 'intelligent' brute force attacks possible.
- Successful exploitation of this vulnerability could enable an attacker to gain access to a user's account (allowing manipulation of the victim user's bets/funds).

### SAFER

- We are not aware of any solutions for this issue.

---

## AmTote Homebet World Accessible Log Vulnerability

---

**Released** September 28, 2001

**Affects** AmTote Homebet

**Reference** <http://www.securityfocus.com/cgi-bin/vulns-item.pl?section=info&id=3370>

### Problem

- Homebet stores all account and corresponding PIN numbers in the homebet.log file. This file is a plaintext file stored in the Homebet virtual directory.
- On a default installation of the Homebet software, the homebet.log file is world readable and accessible to any user across the Internet. This could allow a malicious user to steal the log file and strip out the account and PIN numbers.

### SAFER

- As a workaround, users can change the ACL on the homebet.log file to deny access to the IUSER and other anonymous accounts. We are not aware of any vendor-supplied solutions for this issue.

---

## OpenSSH Key Based Source IP Access Control Bypass Vulnerability

---

**Released** September 26, 2001

**Affects** OpenSSH 2.5, 2.5.1, 2.5.2 and 2.9

**Reference** <http://www.securityfocus.com/cgi-bin/vulns-item.pl?section=info&id=3369>

### Problem

- One of the features offered by OpenSSH is the ability to implement access control based on source IP per key. There exists a bug in this feature that may allow for attackers to bypass some access control and login from unauthorized hosts.
- The access control information is stored with each key in the 'authorized\_keys2' file present in each user's OpenSSH '.ssh' directory. The hosts permitted to login for each key can be specified using the 'from=' directive.
- When two keys of different types appear successively in the '.authorized\_keys2' file, a bug in OpenSSH causes the key options of the second to be applied to the first. Among those options is the access control information.
- Depending on the order of keys, it may be possible for attackers to bypass key-based access control.

### SAFER

- The OpenSSH development team has released an upgrade as well as a source code patch.

---

## Microsoft Exchange OWA Server Resource Starvation Vulnerability

---

**Released** September 26, 2001

**Affects** Microsoft Exchange Server 2000 and 2000 SP1

**Reference** <http://www.securityfocus.com/cgi-bin/vulns-item.pl?section=info&id=3368>

### Problem

- When processing client access requests, OWA Server does not place limits on folder depth. Remote attackers can exploit this to cause a denial of service by requesting access to complex folder structures (which need not exist).
- The CPU and memory consumed while processing these requests may result in a denial of service on the server. Since this is a resource exhaustion attack, all other processes on the system (other services) will be affected.
- The denial of service condition will cease once OWA server has finished processing the request. Repeated attacks can cause a prolonged denial of service.
- To exploit this vulnerability, an attacker must authenticate as a legitimate client.

### SAFER

- Microsoft has released a patch (post SP1).

---

## RedHat Setserial Init Script Predictable Temporary File Vulnerability

---

**Released** September 26, 2001

**Affects** RedHat Linux 7.1

**Reference** <http://www.securityfocus.com/cgi-bin/vulns-item.pl?section=info&id=3367>

### Problem

- A problem with the serial port support in the distribution could make it possible for a user to overwrite arbitrary files. This could result in a denial of service.
- The problem is related to the creation of temporary files, and occurs only under certain circumstances. If a user has recompiled their kernel to enable modular serial support in the kernel, and the rc.serial script has been copied to /etc/rc.d/init.d/serial, the system is vulnerable to a race condition error.
- When executed, the serial init script creates temporary files in a predictable manner. As these scripts are executed with root privileges during system bootstrap, it may be possible for a user to overwrite root-owned files. By guessing the name of a future temporary file, and creating a symbolic link, a user can overwrite the file at the end of the symbolic link.
- This makes it possible for attackers to deny service to other users of the system and potentially gain elevated privileges.

### SAFER

- The Red Hat supplied workaround for this issue is to either: Use a Red Hat supplied kernel, If the kernel must be recompiled, make serial support part of the kernel (versus modular), Under no circumstance should the init script supplied with setserial be used. The following command is recommended by Red Hat to disable the setserial init script: /sbin/chkconfig serial off.

---

## Cisco PIX Firewall SMTP Content Filtering Evasion Vulnerability Re-Introduction

---

**Released** September 26, 2001

**Affects** Cisco PIX Firewall 4.4(7.202), 4.4(4), 5.1(4.206), 5.2(3.210) and 6.0(1)

**Reference** <http://www.securityfocus.com/cgi-bin/vulns-item.pl?section=info&id=3365>

### Problem

- In the case of SMTP, PIX firewalls can be configured so only certain SMTP commands can be allowed through (for example, dropping extra functionality, such as HELP or commands that could be a security concern, like EXPN or VRFY).
- An old vulnerability that allowed for bypassing of this filtering has been re-introduced into PIX firmware. This vulnerability is archived in the SecurityFocus vulnerability database as Bugtraq ID: 1698.
- Exploitation of this vulnerability may allow for remote attackers to send possibly malicious commands to an SMTP server behind the firewall.

### SAFER

- Cisco has released firmware upgrades.

---

## SLRN Arbitrary Shell Script Execution Vulnerability

---

**Released** September 26, 2001

**Affects** slrn 0.9.6.2

**Reference** <http://www.securityfocus.com/cgi-bin/vulns-item.pl?section=info&id=3364>

### Problem

- A problem has been discovered in the program that could allow the execution of arbitrary commands on systems using the vulnerable reader. This could lead to a remote user gaining unauthorized access.
- The problem is in the shell script handling code of slrn. When slrn downloads posts to an NNTP server it attempts to decode binaries automatically. In this process, slrn will attempt to execute any shell scripts contained in the post.
- This could lead to arbitrary commands being executed on the local system. These commands would be executed with the privileges of the slrn user.
- This is currently known to affect only Debian Linux.

### SAFER

- Fixes are available.

---

## PHPNuke Remote File Copy Vulnerability

---

**Released** September 25, 2001

**Affects** PHP-Nuke 1.0 up to 5.2a

**Reference** <http://www.securityfocus.com/cgi-bin/vulns-item.pl?section=info&id=3361>

### Problem

- PHP Nuke contains a vulnerability that may allow for remote attackers to overwrite files with custom data on target web servers. The vulnerability lies in an administrative component of the package, 'admin.php'.
- When the script is requested with a value set for the 'upload' variable, it attempts a file copy using remotely supplied HTML variables as the source and destination files. The script does not ensure that the user requesting the operation is an administrator. As a result, it is possible for remote users to overwrite arbitrary webserver writeable files with data from arbitrary webserver readable files. It is also possible to place arbitrary files in webserver writeable directories on the target filesystem.  
Furthermore, remote attackers can upload files to the webserver. An attacker may be able to upload a custom file to the webserver, then overwrite an arbitrary webserver-writeable file with its contents.
- The destination file does not need to be in the webroot tree.
- This vulnerability may allow for an attacker to gain access to the host, cause denial of service or deface the target website.
- Versions of PostNuke, a derivative of PHP Nuke, are also reportedly vulnerable.

### SAFER

- An unofficial fix has been suggested by Magnus Skjegstad <magnus@skjegstad.com>: In "admin.php"; change "if(\$upload) {" to "if ((\$upload) && (\$admintest)) {" . We are not aware of any vendor-supplied solutions for this issue.

---

## Michael Barretto CardBoard Remote Command Execution Vulnerability

---

**Released** September 25, 2001

**Affects** Michael Barretto CardBoard 2.4

**Reference** <http://www.securityfocus.com/cgi-bin/vulns-item.pl?section=info&id=3360>

### Problem

- Due to the improper filtering of certain types of user-supplied input, it is possible for a user to submit a greeting card which causes arbitrary commands to be executed on the host with privileges of the server.
- This is achievable by specifying arbitrary characters in the recipient field. The user must then send the greeting card. CardBoard insufficiently sanitizes input from untrusted sources. For example, an attacker can use shell metacharacters (';', '|', etc.), which will allow arbitrary commands to be executed by the host with the privileges of the webserver process.
- Successful exploitation of this vulnerability could lead to a complete compromise of the host.

### SAFER

- We are not aware of any solutions for this issue.

---

## H-Sphere Arbitrary File Disclosure Vulnerability

---

**Released** September 25, 2001

**Affects** Positive Software H-Sphere 1.5, 2.0, 2.05, 2.06

**Reference** <http://www.securityfocus.com/cgi-bin/vulns-item.pl?section=info&id=3359>

### Problem

- H-Sphere does not filter '../' sequences from some requests, which has the potential to cause disclosure of sensitive information. A malicious user may construct a specially crafted web request which will allow them to break out of wwwroot and browse the filesystem at large. This is accomplished by using '../' character sequences as a value for the "template\_name" variable.
- For example:
- [http://www.target.com/somepath/psoft.hsphere.CP/somepath/?template\\_name=../../../../../../../../../../../../../../../../etc/passwd](http://www.target.com/somepath/psoft.hsphere.CP/somepath/?template_name=../../../../../../../../../../../../../../../../etc/passwd)
- [http://www.target.com/shiva/psoft.hsphere.CP/admin/2628\\_0/?template\\_name=../../../../../../../../../../../../../../../../etc/passwd](http://www.target.com/shiva/psoft.hsphere.CP/admin/2628_0/?template_name=../../../../../../../../../../../../../../../../etc/passwd)
- Arbitrary web-readable files may be displayed by the attacker using this attack.
- To successfully exploit this issue, the malicious user must have access to an account for a hosted website.

### SAFER

- We are not aware of any solutions for this issue.

---

## Intershop Communications Intershop Arbitrary Command Execution Vulnerability

---

**Released** September 24, 2001

**Affects** Intershop Communications Intershop 4

**Reference** <http://www.securityfocus.com/cgi-bin/vulns-item.pl?section=info&id=3356>

### Problem

- A vulnerability exists in Intershop which could enable a remote user to execute arbitrary commands on a host.
- Submitting a specially crafted URL by way of 'buy.storefront', could result in the execution of arbitrary commands. It is also possible to disclose web directories via this vulnerability.
- Successful exploitation of this vulnerability could lead to the disclosure of private data, and possibly the complete compromise of a target host.

### SAFER

- We are not aware of any solutions for this issue.

---

## Hylafax Hostname Format String Vulnerability

---

**Released** September 23, 2001

**Affects** Hylafax 4.1

**Reference** <http://www.securityfocus.com/cgi-bin/vulns-item.pl?section=info&id=3357>

### Problem

- A problem in the Hylafax software may allow local users to gain elevated privileges under some circumstances. This could also lead to further system compromise, and potentially administrative access.
- The problem is in the hostname handling code of some Hylafax programs. Hylafax does not sufficiently check or sanitize input from users entering a hostname with some programs. Therefore, it's possible to pass a format string to the program, which could be used to execute arbitrary code.
- The problem is known to affect the faxrm and faxalter programs. It is believed that this vulnerability may lie in code shared by both utilities.
- This problem is not present in most implementations, as Hylafax is typically installed without setuid privileges. However, it is implemented as a setuid uucp program on some systems, which makes it possible to gain local privilege elevation

### SAFER

- We are not aware of any solutions for this issue.

---

## Baltimore Technologies MAILsweeper Script Filtering Bypass Vulnerability

---

**Released** September 22, 2001

**Affects** MAILsweeper for SMTP 4.2, 4.2.1 and 4.2.5

**Reference** <http://www.securityfocus.com/cgi-bin/vulns-item.pl?section=info&id=3355>

### Problem

- MAILsweeper does not adequately filter script code from HTML-enabled e-mail. It is possible to use HTML-encoded characters to trick MAILsweeper's filter. Also, adding an additional "<" to the beginning of a HTML tag which includes script code will be sufficient to bypass the script filter.
- These examples will cause script code to be executed:
- <A HREF="ja&#118;ascript:alert('This part should be filtered')">Click here</A>
- <IMG SRC="ja&#118;ascript:alert('This part should be filtered')">
- <<IMG SRC="javascript:alert('This part should be filtered')">
- Successful exploitation may allow malicious code to be executed on client systems receiving HTML e-mail. This is due to the fact that the malicious e-mail will not be filtered at the gateway level and may affect users within an organization that is using MAILsweeper to filter e-mail content.

### SAFER

- The vendor has addressed this issue in version MAILsweeper for SMTP version 4.2.6.

---

## Xcache Path Disclosure Vulnerability

---

**Released** September 21, 2001

**Affects** Xcache Technologies Xcache 2.0 and 2.1

**Reference** <http://www.securityfocus.com/cgi-bin/vulns-item.pl?section=info&id=3352>

### Problem

- Xcache is a dynamic content caching application which runs in conjunction with Microsoft Internet Information Server. Xcache allows for individual pages or entire folders to have caching disabled if necessary. It intercepts all incoming HTTP requests to the webserver and serves any cached pages without involving the webserver in order to increase performance. If a request is made for a page that is not cached by Xcache, it passes the request on to the IIS server for processing.
- When a request is made to the webserver for a page or a page within a folder that is not cached, Xcache returns the full path to the page within the HTTP header information. This path information will be returned regardless of where the page resides on the server.
- This information could potentially be used by an attacker to aid with another attack, such as a directory traversal.

### SAFER

- Xcache Technologies has produced a patch to address this issue, however, it is not available for public download. Users of Xcache can obtain the patch by contacting support@xcache.com.

---

## Half-Life Client Side Connect Buffer Overflow Vulnerability

---

**Released** September 20, 2001

**Affects** Valve Software Half-Life 1.1.0.8

**Reference** <http://www.securityfocus.com/cgi-bin/vulns-item.pl?section=info&id=3353>

### Problem

- A problem in the software package could allow a malicious server to execute arbitrary code. This could allow unauthorized local access.
- The problem is in the /Connect command. This command is used by a client to negotiate a connection with a server on a specific IP address and port. A buffer overflow in this command occurs when 128 bytes or more of data have been received.
- This problem is compounded by the fact that it's possible for a remote server to execute commands on the client. A server may execute the /Connect command on a client through utilities such as the Admin-Mod. An administrator with malicious intent could alter the Admin-Mod source to execute arbitrary commands when vulnerable clients attempted to connect, and thus give the malicious administrator access to the system with the same privileges of the user of the Half-Life client.

### SAFER

- We are not aware of any solutions for this issue.

---

## Pi-Soft SpoonFTP Directory Traversal Vulnerability

---

**Released** September 20, 2001

**Affects** Pi-Soft SpoonFTP 1.1

**Reference** <http://www.securityfocus.com/cgi-bin/vulns-item.pl?section=info&id=3351>

### Problem

- Authenticated users can gain read access to the directories of the host where the FTP server has been installed. Through the use of triple dot '...' sequence when submitting a 'cd' command, arbitrary directories and files could be disclosed, potentially compromising the privacy of user data and/or obtaining information which could be used to further compromise the host's security.
- If successfully exploited this vulnerability could lead to the disclosure of sensitive information assisting in further attacks against the host.

### SAFER

- The vendor has addressed this issue in SpoonFTP 1.1.0.1.

---

## Lotus Domino Internal IP address Disclosure Vulnerability

---

**Released** September 20, 2001

**Affects** Lotus Domino 5.0.8

**Reference** <http://www.securityfocus.com/cgi-bin/vulns-item.pl?section=info&id=3350>

### Problem

- If a specially formed GET request, a path segment comprised of numerous '/' characters, is submitted to the target Domino server. Lotus Domino will reveal the internal IP address of the server. Further technical details are forthcoming.

### SAFER

- Workaround: It is possible to contain the internal IP address of a Lotus Domino server by including 'DominoNoBanner=1' to notes.ini. We are not aware of any vendor-supplied solutions for this issue.

---

## IBM WebSphere Application Server Predictable Session ID Vulnerability

---

**Released** September 19, 2001

**Affects** IBM WebSphere

**Reference** <http://www.securityfocus.com/cgi-bin/vulns-item.pl?section=info&id=3349>

### Problem

- IBM WebSphere Application Server uses predictable sequence numbers for session IDs when issuing cookies to users. Specifically, IBM WebSphere cycles through a limited range of possibilities when determining the sequence number to use for a session ID.
- This is an example of a sequence number: TWG111YAAACVQPQ3UUSZQV2l xxxx y
- The sequence number is based on two counters, xxxx and y, with the rest of the session ID being static. xxxx and y must be alphanumeric characters. The first counter increases incrementally based on the system clock. The last character of the first counter (xxxx) has been determined to be Y, I, A or Q approximately 95% of the time. The second counter (y) will increase by two per request. Since most of the session ID is static and those characters that are variable are not entirely random, this makes it a trivial task to guess the session ID after only a limited number of attempts.
- If this issue is successfully exploited then it is possible for an attacker to obtain the cookie-based authentication credentials for other users, allowing unauthorized access to the vulnerable application.

### SAFER

- The vendor has released a patch which addresses this issue.

---

## John E. Davis MOST Buffer Overflow Vulnerability

---

**Released** September 18, 2001

**Affects** John E. Davis MOST 4.4, 4.41, 4.5, 4.6, 4.7, 4.9.0 and 4.9.1

**Reference** <http://www.securityfocus.com/cgi-bin/vulns-item.pl?section=info&id=3347>

### Problem

- An exploitable buffer overflow exists in MOST. This is due to improper bounds checking of two array variables in the tab expansion of MOST. It is possible for a remote or a local attacker to create a file which, when viewed by MOST, will cause arbitrary code to be executed on the host. This is accomplished by using a malicious file to overwrite stack variables (including the return address). Arbitrary code will be executed as the UID of the user running MOST.
- Successful exploitation could allow a remote attacker to gain local access to a host or allow a local attacker to gain elevated privileges.

### SAFER

- Updates are available.

---

## ZyXel Prestige 642R Router WAN Port Filter Bypass Vulnerability

---

**Released** September 18, 2001

**Affects** ZyXEL Prestige 642R

**Reference** <http://www.securityfocus.com/cgi-bin/vulns-item.pl?section=info&id=3346>

### Problem

- ZyXel Prestige Routers allow administrators to filter ports on both the WAN and LAN interfaces. By default, the filters are set to block WAN IP addresses access to the Telnet administration interface on TCP port 23, and FTP access on TCP port 21.
- An administrator can also set up a filter on the LAN interface in order to block internal network users from accessing these administration interfaces.
- The WAN interface does not filter internal IP addresses from these ports, however, allowing an internal attacker to access the administration interface by connecting to the router's WAN IP address.
- It is important to note that this vulnerability can only be exploited by a malicious user who has gained access to the internal network.

### SAFER

- As a workaround, users can set the router to use Bridge mode.

---

## Oracle 9i Application Server Path Revealing Vulnerability

---

**Released** September 17, 2001

**Affects** Oracle 9i Application Server

**Reference** <http://www.securityfocus.com/cgi-bin/vulns-item.pl?section=info&id=3341>

### Problem

- A vulnerability exists that could allow a malicious user to view the full path to the web folder. If the malicious user were to send the Oracle 9i AS an HTTP request for a non-existent .jsp file, the server would return an error page containing path information to the web folder.
- An HTTP request for <http://target.com/folder/java/unknown.jsp> would yield an error message containing a path similar to: `c:\oracle\ias\apache\apache\htdocs\target\folder\java\jsp\unknown.jsp`
- A similar vulnerability was found in Apache Tomcat 3.1 which may be related to this vulnerability. See BugTraq ID 1531 for details.

### SAFER

- As a solution to this problem, Oracle recommends upgrading to OJSP 1.1.2.0.0.

---

## Computer Associates ARCServe Cleartext Administrative Password Vulnerability

---

**Released** September 16, 2001

**Affects** ARCServe 6.61, 2000 and 2000 Advanced Edition 7.0

**Reference** <http://www.securityfocus.com/cgi-bin/vulns-item.pl?section=info&id=3343>

### Problem

- ARCServe stores its administrator account and password, in clear text, in `\ARCSERVE$DR\<TARGET_SERVER>\aremote.dmp`.
- Since the account performing backups is able to access system files, and may be configured to run under the NT domain administrator's account, an attacker able to read this file can gain administrative access to the host.

### SAFER

- Limit access to the ARCSERVE\$ network share to the backup account and domain administrator. We are not aware of any vendor-supplied solutions for this issue.

---

## Computer Associates ARCServe Insecure Default Network Share Vulnerability

---

**Released** September 16, 2001

**Affects** ARCServe 6.61, 2000 and 2000 Advanced Edition 7.0

**Reference** <http://www.securityfocus.com/cgi-bin/vulns-item.pl?section=info&id=3342>

### Problem

- Versions of this product contain an insecure default install configuration which leaves an open network share, 'ARCSERVE\$', available to any user in the domain.
- Access to this share can allow malicious users to read sensitive system data, or to overwrite files critical to backup operations.
- Note that another vulnerability in connection with this product (CA ARCServe Cleartext Administrative Password Vulnerability) could amplify the effects of this vulnerability.

### SAFER

- Workaround: allow only the backup account and the administrator access to the 'ARCSERVE\$' share. Computer Associates have released a patch for Windows NT 4.0/Windows 2000 w/SP2a.

---

## WebDiscount E-Shop Remote Arbitrary Command Execution Vulnerability

---

**Released** September 15, 2001

**Affects** Michael Boehme WebDiscount E-Shop Online-Shop System 1.0

**Reference** <http://www.securityfocus.com/cgi-bin/vulns-item.pl?section=info&id=3340>

### Problem

- A problem exists in a default implementation of the software that may allow a user to potentially pass malicious input to the script. This is due insufficient sanitization from untrusted sources. For example, an attacker can use shell metacharacters (';', '|', etc.), which will allow arbitrary commands to be executed by the host with the privileges of the webserver process.
- An example of a malicious web request: host/cgi-bin/eshop.pl?seite=;ls|
- Successful exploitation of this issue may cause sensitive information to be disclosed to the attacker.

### SAFER

- We are not aware of any solutions for this issue.

---

## Microsoft Index Server 2.0 File Information and Path Disclosure Vulnerability

---

**Released** September 14, 2001

**Affects** Microsoft Index Server 2.0

**Reference** <http://www.securityfocus.com/cgi-bin/vulns-item.pl?section=info&id=3339>

### Problem

- Malicious users could send specifically crafted HTTP request to an Internet Information Services server running Index Server to reveal path information, file attributes, and possibly some lines of the file contents.
- The sqlqhit.asp file is located in the \inetpub\iissamples\ISSamples\ folder and is installed by default.

### SAFER

- We are not aware of any solutions for this issue.

---

## Counterpane Password Safe Data Buffer Recovery Vulnerability

---

**Released** September 13, 2001

**Affects** Counterpane Password Safe 1.7.1

**Reference** <http://www.securityfocus.com/cgi-bin/vulns-item.pl?section=info&id=3337>

### Problem

- A problem in the program could make it possible for local users to gain access to clear text information that may be sensitive. This information could contain usernames and/or passwords. The problem is in the management of memory when the program is minimized.
- The program features an option that when minimized, will clear any passwords from the clipboard. However, when the program is minimized, Windows copies the password to a buffer. This buffer may be accessed by a local user to extract the password or username.
- This problem makes it possible for a local user to gain access to usernames and/or passwords in system memory, and may lead to compromise of computing resources.

### SAFER

- We are not aware of any solutions for this issue.

---

## Check Point Firewall-1 GUI Log Viewer Vulnerability

---

**Released** September 12, 2001

**Affects** Firewall-1 4.0 up to SP8, 1.4.1 up to SP5, Check Point Software Next Generation

**Reference** <http://www.securityfocus.com/cgi-bin/vulns-item.pl?section=info&id=3336>

### Problem

- It has been reported that Firewall-1 may contain a buffer overflow vulnerability. The vulnerability is allegedly in logging of authentication attempts by GUI log viewing clients. If a supplied username is excessive in length, an overflow may occur when the username is logged with a length warning.
- It may be possible for remote attackers to execute arbitrary code as root on systems running Firewall-1. The attack must be launched from hosts that are permitted to view logs via the GUI interface.

### SAFER

- Check Point has made hotfixes available.

---

## Red Hat Linux Apache Remote Username Enumeration Vulnerability

---

**Released** September 12, 2001

**Affects** RedHat Linux 7.0

**Reference** <http://www.securityfocus.com/cgi-bin/vulns-item.pl?section=info&id=3335>

### Problem

- Versions of Apache webserver shipping with Red Hat Linux 7.0, (and possibly other Apache distributions) install with a default misconfiguration which can permit remote users to determine whether a given username exists on the vulnerable system.
- When a remote user submits an HTTP request for a possible user's default home page, the server has one of three responses.
- In a case where the tested username is valid, and that account has been configured with a homepage, the server replies with HTTP result code 200, and the user's homepage.
- Alternatively, when the tested username does exist on the system, but does not have a homepage, the server responds with HTTP result code 403, and the server message "You don't have permission to access /~username on this server."
- However, if the tested username does not exist as an account on the system, the Apache server's response is HTTP result code 404 and the message "The requested URL /~username was not found on this server."
- Because the server responds differently in the latter two cases, a remote user can test and enumerate possible usernames. Properly exploited, this information could be used in further attacks on the vulnerable host.

### SAFER

- Workarounds are available. We are not aware of any vendor-supplied solutions for this issue.

---

## Microsoft Outlook Express 6 Plain Text Message Script Execution Vulnerability

---

**Released** September 12, 2001

**Affects** Microsoft Outlook Express 6.0

**Reference** <http://www.securityfocus.com/cgi-bin/vulns-item.pl?section=info&id=3334>

### Problem

- The content-type field in the header is used by email clients and gateway filtering software to determine how to handle the message. Many administrators use gateway software to filter mail of content-type text/html so that messages containing potentially malicious scripts are not delivered.
- A vulnerability exists in Outlook Express 6 which may lead to code embedded in an email message of content-type 'text/plain' to be executed.
- The script code must be contained within the first 57 characters on the first line of the message. Any additional characters on either line will cause the message to be parsed in plain text. It is not known why this behaviour is present.
- Only the <script> tag appears to function in this manner.
- It is important to note that Outlook Express 6 does not allow any scripting to be executed by default. This security feature must be turned off in order to exploit this vulnerability.

### SAFER

- A workaround is to disable scripting in Outlook Express. We are not aware of any vendor-supplied solutions for this issue.

---

## EFTP Server Directory and File Existence Vulnerability

---

**Released** September 12, 2001

**Affects** Khamil Landross and Zack Jones EFTP 2.0.7.337

**Reference** <http://www.securityfocus.com/cgi-bin/vulns-item.pl?section=info&id=3333>

### Problem

- Users can confirm the existence and location of various files and directory structures outside the FTP root through a trial and error method. EFTP improperly restricts access outside of the FTP root when modified time (mdtm) and size (size) commands are used. The modified time command returns the last modified time of the requested file. The size command returns information on the size of the given file.
- Submitting a 'size' or 'mdtm' command for a file outside of the FTP root could disclose directory structure information of unpublished filesystems on the host. If the requested command is fulfilled by the vulnerable service, the attacker can confirm the relative path to the file.
- Successful exploitation of this vulnerability could lead to the disclosure of sensitive information and may aid in the execution of future attacks.

### SAFER

- We are not aware of any solutions for this issue.

---

## EFTP Clear Text Password Storage Vulnerability

---

**Released** September 12, 2001

**Affects** Khamil Landross and Zack Jones EFTP 2.0.7.337

**Reference** <http://www.securityfocus.com/cgi-bin/vulns-item.pl?section=info&id=3332>

### Problem

- EFTP stores all usernames and passwords in the file \Program Files\leftp2\leftp2users.dat in clear text. If a malicious user were to gain access to this file, they would have a list of all usernames and their associated passwords.

### SAFER

- We are not aware of any solutions for this issue.

---

## EFTP Password Hash Retrieval Vulnerability

---

**Released** September 12, 2001

**Affects** Khamil Landross and Zack Jones EFTP 2.0.7.337

**Reference** <http://www.securityfocus.com/cgi-bin/vulns-item.pl?section=info&id=3331>

### Problem

- EFTP Server supports the use of UNC shares. UNC shares are a way for users to identify shared resources, '/' or '\\' specifies the server and '/' or '\' reveals the path to the shared resource. A UNC name format is structured similar to this: \\server\share\path\filename
- A flaw in EFTP Server could allow a user to lead the server into disclosing the credentials of the user the server is running under.
- If a logged in FTP user connects to an external share and submits a malformed 'list' command, the user could force the FTP server to make an external SMB connection to a host of his choice. A likely connection would be to a malicious host expecting the connection. In order for the server to successfully connect to the host, the server would have to provide the login credentials of the user the server is running under. A password hash is sent across the external connection to the host. This information could easily be captured by a third party network utility listening for internal and external traffic on the host. The captured password hash could be resolved into the username and password.
- If an attacker successfully exploited this vulnerability it could assist in further attacks against the host, and possibly lead to complete compromise of the host.

### SAFER

- We are not aware of any solutions for this issue.

---

## RSA BSAFE SSL-J Authentication Bypass Vulnerability

---

**Released** September 12, 2001

**Affects** RSA Security BSAFE SSL-J SDK 3.0, 3.0.1 and 3.1, Cisco iCDN 2.0

**Reference** <http://www.securityfocus.com/cgi-bin/vulns-item.pl?section=info&id=3329>

### Problem

- Under certain conditions, if an error occurs during the SSL client-server handshake, the SSL session key may be stored in a cache rather than being discarded. Once cached, this session key can be used by an attacker to cause a server to skip the full client authentication scheme, using a much shorter one. This effectively allows the attacker to fully bypass the client authentication.
- On systems that rely solely on the authentication mechanism provided by SSL, this could enable an attacker to perform unauthorized actions. Additional technical details are forthcoming.

### SAFER

- RSA BSAFE SSL-J customers with active maintenance agreements and who currently use an affected version of RSA BSAFE SSL-J are recommended to upgrade to the latest release version of RSA BSAFE SSL-J. This issue is known to affect version 2.0 of Cisco's iCDN, and has been fixed in version 2.0.1.

---

## Textor Webmasters Limited ListRec.pl Input Validation Vulnerability

---

**Released** September 12, 2001

**Affects** Textor Webmasters Ltd listrec.pl 1.0

**Reference** <http://www.securityfocus.com/cgi-bin/vulns-item.pl?section=info&id=3328>

### Problem

- 'listrec.pl' does not adequately validate user-supplied input. It is possible for an attacker to craft a malicious web request which will cause remote commands to be executed on the host (with the privileges of the webserver process). This is due to the fact that 'listrec.pl' does not filter shell metacharacters (such as ';' or '|') from web requests.
- Additionally, because of the nature of insufficient input validation, it may be possible for a remote attacker to view arbitrary web-readable files via a directory traversal attack. This would be accomplished by using './.' sequences (or some variation) to break out of wwwroot and browse the filesystem of the host.

### SAFER

- We are not aware of any solutions for this issue.

---

## Trend Micro InterScan eManager Buffer Overflow Vulnerability

---

**Released** September 12, 2001

**Affects** Trend Micro InterScan eManager 3.51 and 3.51j

**Reference** <http://www.securityfocus.com/cgi-bin/vulns-item.pl?section=info&id=3327>

### Problem

- Several CGI components of eManager contain a buffer overflow vulnerability which could allow an attacker to execute arbitrary code within the Local System context. When a buffer overflow occurs, it allows the user to overwrite stack variables, including the return address.
- The vulnerable modules are:
  - /eManager/cgi-bin/register.dll
  - /eManager/Content%20Management/ContentFilter.dll
  - /eManager/Content%20Management/SFNofitication.dll
  - /eManager/Email%20Management/cgi-bin/register.dll
  - /eManager/Email%20Management/cgi-bin/TOP10.dll
  - /eManager/Email%20Management/cgi-bin/SpamExcp.dll
  - /eManager/Email%20Management/cgi-bin/spamrule.dll
- It is important to note the web management console does not have an authentication method.

### SAFER

- As a workaround, users could disable the web management console, or enable NTLM authentication through the Internet Service Manager for the console. Trend Micro has released a patch to address this vulnerability for the Japanese version of eManager.

---

## SpeechD Privileged Command Execution Vulnerability

---

**Released** September 11, 2001

**Affects** SpeechD 0.1 and 0.2

**Reference** <http://www.securityfocus.com/cgi-bin/vulns-item.pl?section=info&id=3326>

### Problem

- SpeechD has been found to contain an input validation flaw under certain implementations. User input is accepted and passed to a system() call without having been checked for shell metacharacters. This can permit a local user to pass arbitrary commands to be executed at the privilege level of speechd by passing them to the /dev/speech device.
- This issue has been confirmed to affect speechd running with the rsynth application. It may also potentially affect festival and other applications.

### SAFER

- Workaround is available. We are not aware of any vendor-supplied solutions for this issue.

---

## Apple Macintosh OS X FBCIndex File Contents Disclosure Vulnerability

---

**Released** September 11, 2001

**Affects** Apple MacOS X 10.0 up to 10.0.4

**Reference** <http://www.securityfocus.com/cgi-bin/vulns-item.pl?section=info&id=3325>

### Problem

- A remote attacker may read sorted listings of data stored in files by submitting a URL to the vulnerable host's web service of the following form:  
`http://www.example.com/target_directory/.FBCIndex.`
- This information could provide an attacker with sensitive information including potential passwords useful in dictionary attacks, system configuration, installed applications, etc. Properly exploited, this information could allow an attacker to further compromise the security of the host.

### SAFER

- Temporary workaround is to restrict remote access to .FBCIndex files. We are not aware of any vendor-supplied solutions for this issue.

---

## Apple Macintosh OS X .DS\_Store Directory Listing Disclosure Vulnerability

---

**Released** September 11, 2001

**Affects** Apple MacOS X 10.0 up to 10.0.4

**Reference** <http://www.securityfocus.com/cgi-bin/vulns-item.pl?section=info&id=3324>

### Problem

- Each directory in the filesystem can contain a hidden object, ".DS\_Store" containing data which includes a list of files stored there. This object is created when a local user views a given directory using the Finder.
- A remote attacker may read this directory content information by submitting a URL to the vulnerable host's web service of the following form:  
`http://www.example.com/target_directory/.DS_store.`
- This information could provide an attacker with sensitive information including system configuration, installed applications, etc. Properly exploited, this information could allow an attacker to further compromise the security of the host.

### SAFER

- Temporary workaround is to disallow remote access to .DS\_store files. We are not aware of any vendor-supplied solutions for this issue.

---

## NetOp School Administration Authentication Vulnerability

---

**Released** September 11, 2001

**Affects** CrossTec Corp NetOp School 1.5

**Reference** <http://www.securityfocus.com/cgi-bin/vulns-item.pl?section=info&id=3321>

### Problem

- NetOp School is classroom software that allows an instructor to view, control, and broadcast to student terminals.
- When the student logs in to the terminal, the student component of the software runs in the background. If the student then attempts to start the administrator component, they will be challenged for authentication.
- However, if the student uses a task manager to terminate the student process, they can start the administrator software without being prompted for authentication.
- This could allow an attacker to browse any other terminals in the classroom network.

### SAFER

- We are not aware of any solutions for this issue.

---

## Digital Unix MSGCHK MH\_PROFILE Symbolic Link Vulnerability

---

**Released** September 10, 2001

**Affects** Digital (Compaq) TRU64/DIGITAL UNIX 4.0d, 4.0e, 4.0f and 4.0g

**Reference** <http://www.securityfocus.com/cgi-bin/vulns-item.pl?section=info&id=3320>

### Problem

- msgchk fails to check file permissions before opening user configuration files in the user's home directory. As a result, the user may create a symbolic link between the .mh\_profile configuration file and a target file. Because root privilege is maintained on reading the config file, and symbolic links are followed, a local user is able to read the first line of data contained in any target file readable by the msgchk user. Since msgchk runs setuid root in some implementations, this allows limited information to be read from any file on the host.

### SAFER

- Temporary workaround: Unless msgchk must be run suid, (i.e. for support of "rpop"), strip the suid bit (chmod u-s /usr/bin/mh/msgchk). We are not aware of any vendor-supplied solutions for this issue.

---

## Leon J Breedt Pam-PSQL Remote SQL Query Manipulation Vulnerability

---

**Released** September 10, 2001

**Affects** Leon J Breedt pam-pgsql 0.5.1

**Reference** <http://www.securityfocus.com/cgi-bin/vulns-item.pl?section=info&id=3319>

### Problem

- 'pam-psql' is prone to a vulnerability which will allow SQL queries to be manipulated via any medium which requires a user to authenticate (HTTP, SSH, telnet, etc). Data that is included in SQL query strings is not adequately sanitized. It may be possible for users to modify the structure of SQL queries by carefully constructing variables containing metacharacters that will be included in the target query.
- This issue allows the user to access resources that would normally be restricted, which may in turn provide an opportunity for the attacker to exploit other vulnerabilities that exist in the server. The attacker may be able to exploit this issue to gain unauthorized access to the host.

### SAFER

- We are not aware of any solutions for this issue.

---

## Joerg Wendland Pam-PSQL Remote SQL Query Manipulation Vulnerability

---

**Released** September 10, 2001

**Affects** Joerg Wendland pam-pgsql 0.9.2

**Reference** <http://www.securityfocus.com/cgi-bin/vulns-item.pl?section=info&id=3317>

### Problem

- 'pam-psql' is prone to a vulnerability which will allow SQL queries to be manipulated via any medium which requires a user to authenticate(HTTP, SSH, telnet, etc). Data that is included in SQL query strings is not adequately sanitized. It may be possible for users to modify the structure of SQL queries by carefully constructing variables containing metacharacters that will be included in the target query.
- This issue allows the user to access resources that would normally be restricted, which may in turn provide an opportunity for the attacker to exploit other vulnerabilities that exist in the server. The attacker may be able to exploit this issue to gain unauthorized access to the host.

### SAFER

- The vendor has addressed this issue in a new release.

---

## MacOS X Client Apache Directory Contents Disclosure Vulnerability

---

**Released** September 10, 2001

**Affects** Apache 1.3.14Mac

**Reference** <http://www.securityfocus.com/cgi-bin/vulns-item.pl?section=info&id=3316>

### Problem

- An invisible file (.DS\_Store) is created by the finder, in each web directory. The invisible file contains all of the file contents within that directory.
- Due to a flaw in Mac OS file permissions, an issue exists which could disclose the contents of a particular web directory to an unauthorized user. Requesting a URL with the relative path of a '.DS\_Store' file, will reveal the contents of the particular directory. For example:  
`http://www.example.com/directoryname/.ds_store` will reveal the file contents of the requested directory (directoryname).
- This vulnerability could be used in conjunction with a previously discovered issue (BID 2852), which causes files to be arbitrarily disclosed through mixed case file requests.
- Successful exploitation of this vulnerability could lead to the disclosure of sensitive data, which may assist in further attacks against the target host.

### SAFER

- We are not aware of any solutions for this issue.

---

## NSS NSS\_PostgreSQL Remote SQL Query Manipulation Vulnerability

---

**Released** September 10, 2001

**Affects** Alessandro Gardich nss\_postgresql 0.6.1

**Reference** <http://www.securityfocus.com/cgi-bin/vulns-item.pl?section=info&id=3315>

### Problem

- The NSS database module 'nss\_postgresql' is prone to a vulnerability which will allow SQL queries to be manipulated via a HTTP request. Data that is included in SQL query strings is not adequately sanitized. It may be possible for users to modify the structure of SQL queries by carefully constructing variables containing metacharacters that will be included in the target query.
- It is believed that the attacker would need an interactive account on the vulnerable host to exploit this issue. Attacks will be executed on the database server as the database user that is making the query.
- This issue allows the user to access resources that would normally be restricted, which may in turn provide an opportunity for the attacker to exploit other vulnerabilities that exist in the server.

### SAFER

- We are not aware of any solutions for this issue.

---

## Joerg Wendland LibNSS-PgSQL Remote SQL Query Manipulation Vulnerability

---

**Released** September 10, 2001

**Affects** Joerg Wendland libnss-pgsql 0.9.0

**Reference** <http://www.securityfocus.com/cgi-bin/vulns-item.pl?section=info&id=3314>

### Problem

- The NSS database module 'libnss-pgsql' is prone to a vulnerability which will allow SQL queries to be manipulated via a HTTP request. Data that is included in SQL query strings is not adequately sanitized. It may be possible for users to modify the structure of SQL queries by carefully constructing variables containing metacharacters that will be included in the target query.
- It is believed that the attacker would need an interactive account on the vulnerable host to exploit this issue. Attacks will be executed on the database server as the database user that is making the query.
- This issue allows the user to access resources that would normally be restricted, which may in turn provide an opportunity for the attacker to exploit other vulnerabilities that exist in the server.

### SAFER

- The vendor has addressed this issue in a new release.

---

## Digital Unix MSGCHK Buffer Overflow Vulnerability

---

**Released** September 10, 2001

**Affects** Digital (Compaq) TRU64/DIGITAL UNIX 4.0d, 4.0e, 4.0f and 4.0g

**Reference** <http://www.securityfocus.com/cgi-bin/vulns-item.pl?section=info&id=3311>

### Problem

- A problem has been discovered in versions of Digital Unix (4.0D-4.0G) that could allow a local user to gain elevated privileges. The vulnerability could result in complete system compromise.
- The problem is due to a buffer overflow in msgchk, a component of the message handling system used to check for messages in all known mail drops for a given user.
- If mshcchk is invoked at the command line, accompanied by a string of approximately 8000 bytes, a buffer overflow occurs, allowing the user to overwrite stack variables, including the return address.
- Because the msgchk program runs setuid root, this makes it possible for a local user to gain administrative access to the vulnerable system.

### SAFER

- Temporary workaround: Unless msgchk must be run suid, (i.e. for support of "rpop"), strip the suid bit (chmod u-s /usr/bin/mh/msgchk). We are not aware of any vendor-supplied solutions for this issue.

---

## Taylor UUCP Argument Handling Privilege Elevation Vulnerability

---

**Released** September 08, 2001

**Affects** Ian Lance Taylor Taylor UUCP 1.0.6

**Reference** <http://www.securityfocus.com/cgi-bin/vulns-item.pl?section=info&id=3312>

### Problem

- A problem has been discovered in the Taylor UUCP package that makes it possible for a local user to gain elevated privileges. The problem is in the improper checking of command line input, and acceptance of arbitrary configuration files.
- uux is a program included with the Taylor UUCP package. uux, as implemented in the package, is designed to execute commands remotely on other UUCP hosts, such as rnews and rmail. This program is usually used to provide the mail and news distribution functionality in a UUCP network.
- The problem occurs in handling of configuration files by uux when uucp is invoked within it. By executing uux, and using the uucp program within uux, and passing a malicious configuration file to uucp through the --config parameter, it is possible for a local user to execute commands on a local host with setuid privileges. The commands passed to uucp through the file specified in --config are usually executed by uuxqt, a daemon on the system that by default executes rnews and rmail. uuxqt is setuid uucp.
- Therefore, a local user executing uux, and passing a malicious configuration file to uucp using the config flag, may gain privilege elevation to uucp, and potentially local root access when the configuration file is executed by uuxqt.

### SAFER

- Updates are available.

---

## Check Point Firewall-1 GUI Client Log Viewer Symbolic Link Vulnerability

---

**Released** September 08, 2001

**Affects** Firewall-1 3.0 up to 4.1

**Reference** <http://www.securityfocus.com/cgi-bin/vulns-item.pl?section=info&id=3303>

### Problem

- A problem with Firewall-1 makes it possible for a local user to overwrite critical system files. This could result in a denial of service to legitimate users of the system. The problem of overwriting files occurs when Check Point Firewall-1 is used in Log Viewer mode.
- When a Firewall-1 administrator with access to the administration GUI launches the Log Viewer, and saves a file through the Log Viewer, the user is prompted for a name for the file through the "Save As" function. Firewall-1 does not first check for the existence of the file, and any directory may be specified, which could result in the overwriting of any file ending in the .log extension.
- Additionally, if a user with access to the administrative interface of the firewall also has local access, the user can create a symbolic link with an extension ending in .log, and point the symbolic link to a root owned file. Upon using the Log Viewer with the "Save As" function, and saving the file to the location of the symbolic link, the file at the end of the symbolic link will be overwritten. Since the administrative interface executes with root-level privileges, this could result in a denial of service.

### SAFER

- We are not aware of any solutions for this issue.

---

## SeaGlass Technologies sglMerchant Directory Traversal Vulnerability

---

**Released** September 08, 2001

**Affects** SeaGlass Technologies, Inc sglMerchant 1.0

**Reference** <http://www.securityfocus.com/cgi-bin/vulns-item.pl?section=info&id=3309>

### Problem

- sglMerchant does not adequately filter user-supplied input in the form of '../' sequences. It is possible for a remote attacker to construct a web request which will break out of wwwroot to browse the filesystem of the host. The attacker may exploit this issue to display arbitrary web-readable files.
- For example: `www.server.com/cgi-shop/view_item? HTML_FILE=../../../../..file`
- The sensitive information contained in disclosed files may aid the attacker in making further, more educated attempts at fully compromising the host.

### SAFER

- We are not aware of any solutions for this issue.

---

## Hassan Consulting Shopping Cart Arbitrary Command Execution Vulnerability

---

**Released** September 08, 2001

**Affects** Hassan Consulting Shopping Cart 1.23

**Reference** <http://www.securityfocus.com/cgi-bin/vulns-item.pl?section=info&id=3308>

### Problem

- Shopping Cart does not filter certain types of user-supplied input from web request. This makes it possible for a malicious user to submit a request which causes arbitrary commands to be executed on the host (with the privileges of the webserver process).
- An example of the type of input that is not filtered: `www.server.com/cgi-local/shop.pl/SID=947626980.19094/page=;ls|`
- Sensitive data may be disclosed to a remote attacker as a result of this issue, potentially allowing the attacker to gain local access to the host. The remote attacker will also be able to bypass authentication for the ShopPlus Cart service and access other accounts and restricted information.
- It is important to note that while the user can execute commands, the "../" string is filtered and cannot be used.

### SAFER

- We are not aware of any solutions for this issue.

---

## Check Point Firewall-1 Policyname Temporary File Creation Vulnerability

---

**Released** September 08, 2001

**Affects** Firewall-1 3.0 up to 4.1

**Reference** <http://www.securityfocus.com/cgi-bin/vulns-item.pl?section=info&id=3300>

### Problem

- A problem with Firewall-1 makes it possible for a local user to change permissions of critical system files. This could lead to a denial of service, or potentially elevated privileges. The problem is in the creation of predictable temporary files by the Check Point Firewall-1 package.
- When a user accesses the GUI administration interface of Firewall-1 and makes alterations to rule sets, a file is created in the /tmp directory using the name of the firewall policy as a file name, and an extension of .cpp. This file is created when firewall ruleset compilation occurs, after the ruleset has been edited and committed.
- The file is created with world-writeable permissions, and is owned by root. By creating a symbolic link in the /tmp directory using the name of a firewall policy, and pointing the symbolic link to a file owned by root, the file at the end of the symbolic link will inherit world-writeable permissions.
- This problem makes it possible for a local user to alter system configuration, and potentially gain local root access.

### SAFER

- It is recommended that users of vulnerable software upgrade to minimum revision of Check Point Firewall 4.1 SP4.

---

## Norton AntiVirus for Microsoft Exchange 2000 Information Disclosure Vulnerability

---

**Released** September 07, 2001

**Affects** Symantec Norton AntiVirus for MS Exchange 2.5

**Reference** <http://www.securityfocus.com/cgi-bin/vulns-item.pl?section=info&id=3305>

### Problem

- A problem exists in Microsoft Exchange 2000 when running with Norton AntiVirus for Microsoft Exchange. A host running this combination of software can be tricked into disclosing mail directory paths to an attacker.
- This issue occurs when a message attachment is sent via e-mail to an affected host running Norton AntiVirus for Microsoft Exchange. If the attachment is scanned and rejected then the message will be bounced back to the sender with notification of why the message was rejected. When this happens, the path to the intended recipient's INBOX is sent in the message header of the rejection notification. The expected behavior is that the header in the returned message will only contain the destination address of the user and not the path of the user's INBOX.
- This can be exploited by an attacker who intentionally crafts a message to a user on the host which contains an attachment which will be rejected by the host.

### SAFER

- Workaround is to customize Norton AntiVirus for Microsoft Exchange 2000's notification feature(using 'Global Options') that sends rejected messages back to the sender to not include the mailbox location in the bounced message. We are not aware of any vendor-supplied solutions for this issue.

---

## ProFTPD Client Hostname Resolving Vulnerability

---

**Released** September 07, 2001

**Affects** ProFTPD 1.2 up to 1.2pre9

**Reference** <http://www.securityfocus.com/cgi-bin/vulns-item.pl?section=info&id=3310>

### Problem

- ProFTPD contains a vulnerability that may allow for remote attackers to bypass ProFTPD access control lists (ACLs) or have false information logged.
- When 'UseReverseDNS' mode is set in the configuration file, ProFTPD will attempt to 'reverse resolve' the hostnames of clients connecting. The resolved hostname will then be evaluated against the ACLs and recorded as the client address in the logs. Unfortunately, ProFTPD does not forward resolve the hostname to verify that one of the IP addresses listed in DNS records matches that of the connected client.
- It may be possible for a remote attacker with control over address space to set an arbitrary hostname as the PTR record for the attacking address. When the attacker connects, ProFTPD will resolve the attacker-specified hostname and will evaluate it against its hostname-based ACLs. If the attacker is aware of permitted hostnames, it may be possible to bypass ACL restrictions and login by exploiting this vulnerability. The ProFTPD logs will also record the reverse-resolved hostname.

### SAFER

- A workaround is to disable the 'UseReverseDNS' option in the configuration file. We are not aware of any vendor-supplied solutions for this issue.

---

## Power Up HTML Directory Traversal Arbitrary File Disclosure Vulnerability

---

**Released** September 07, 2001

**Affects** Power Up HTML 0.8033beta

**Reference** <http://www.securityfocus.com/cgi-bin/vulns-item.pl?section=info&id=3304>

### Problem

- The primary scripts in Power Up HTML (r.pl or r.cgi) do not filter ../ requests. This allows a user to construct a HTTP request which could allow disclosure of file contents or code execution. Failure to filter metacharacters from HTTP requests can allow user-supplied values to run.
- In order to view or execute the files, the web service would have to have adequate permission to them.

### SAFER

- We are not aware of any solutions for this issue.

---

## Merit AAA RADIUS Server rlmadmin Symbolic Link Vulnerability

---

**Released** September 07, 2001

**Affects** Merit rladmin 3.8M

**Reference** <http://www.securityfocus.com/cgi-bin/vulns-item.pl?section=info&id=3302>

### Problem

- The 'rlmadmin' user management utility included with the Merit AAA RADIUS Server package is susceptible to a trivial symbolic link attack. The program allows users to specify a directory from which configuration files should be loaded at runtime using the '-d' command-line switch. A help file, 'rlmadmin.help', is loaded from this directory and displayed directly to the user when the program is run.
- The vulnerability exists because the program is setuid root and does not check if the help file is symbolically linked before displaying its contents to the user. As a local user, it is trivial for a local user to read any file on the system. This may lead to the disclosure of sensitive data and system compromise.

### SAFER

- We are not aware of any solutions for this issue.

---

## Microsoft Exchange OWA Global Address List Disclosure Vulnerability

---

**Released** September 06, 2001

**Affects** Microsoft Exchange Server 5.5 up to 5.5SP4

**Reference** <http://www.securityfocus.com/cgi-bin/vulns-item.pl?section=info&id=3301>

### Problem

- Due to a flaw in a component (fumsg.asp) of OWA, it is possible for unauthorized user's to gain read access to the Global Address List.
- Typically when performing a Find Users request, the user interface gathers the necessary information required to complete the search request. This includes confirming that the user making the request has successfully authenticated to the server. Once the information is gathered and confirmed, the user interface calls a back end function (fumsg.asp) to carry out the request. However due to the flaw in OWA, an unauthenticated user can make a search request directly to the back end function (fumsg.asp), circumventing authentication to the Exchange server.
- If successfully exploited, a user could gain read access to the entire Global Address List. Knowledge of this information could assist in further attacks against the target host. Specifically, this information could be used to spam users on the host.

### SAFER

- Microsoft has released a patch which rectifies this issue.

---

## NetBSD semop Arbitrary Code Execution Vulnerability

---

**Released** September 06, 2001

**Affects** NetBSD 1.4 up to 1.5.1 and current pre20010805

**Reference** <http://www.securityfocus.com/cgi-bin/vulns-item.pl?section=info&id=3298>

### Problem

- The problem is due to insufficient length checking on a parameter passed to the semop() function, which acts as the entry point for the semop syscall. The function stores an unsigned integer argument 'nsops' in a local signed variable. This value is then used to copy data from user memory onto the process' kernel stack. The vulnerability exists because it is possible to bypass the check used to ensure that a sane value is given. Passing a large numeric value and causing a signed integer overflow can accomplish this.
- This vulnerability can be used to write an almost arbitrary number of bytes to the process' kernel stack. It could be exploited to cause a kernel trap, call arbitrary kernel code, or execute arbitrary code on an architecture where stack memory is executable.

### SAFER

- Vendor-supplied updates that rectify this issue are available.

---

## Baltimore Technologies WEBSweeper Restricted Directory Disclosure Vulnerability

---

**Released** September 05, 2001

**Affects** Baltimore Technologies WEBSweeper 4.02

**Reference** <http://www.securityfocus.com/cgi-bin/vulns-item.pl?section=info&id=3296>

### Problem

- WEBSweeper enables the administrator to block remote access to specific web directories. A vulnerability exists in WEBSweeper which could enable a remote user to bypass this feature and gain access to restricted web directories. Requesting such a directory along with specially chosen characters (example: '..' '/' '.' '/' '/'), could reveal the contents of the known web directory.
- Successful exploitation of this vulnerability could lead to the disclosure of private/sensitive data, possibly assisting in further attacks against the target host.

### SAFER

- Baltimore Technologies has released a technote document, which suggests that it is not practical to use WEBSweeper to administer URL blacklists. We are not aware of any vendor-supplied solutions for this issue.

---

## GNU Mailman Empty Password Blank Salt Vulnerability

---

**Released** September 05, 2001

**Affects** GNU Mailman 2.0 up to 2.0.5

**Reference** <http://www.securityfocus.com/cgi-bin/vulns-item.pl?section=info&id=3295>

### Problem

- A problem with GNU Mailman could make it possible for a remote user to gain access to list functions as an arbitrary user, or potentially higher privileges. The problem is mainly circumstantial, and involves the existence of a blank hashed password file (zero bytes).
- When a password is entered to permit entry to an access controlled section (for any user), the crypt function attempts to extract the salt of the hash from the adm.pw file. However, if the adm.pw file is zero bytes, the salt returns a blank value. When the password is then hashed with the salt, it too becomes a blank value. When these two values are compared, the result is a positive match for a password, thus permitting access.
- This problem makes it possible for a remote user to gain access to a Mailman user's account, or access Mailman as the administrator of a mailing list.

### SAFER

- Updates are available

---

## ShopPlus Cart Arbitrary Command Execution Vulnerability

---

**Released** September 05, 2001

**Affects** Kabotie Software Technologies ShopPlus Cart 1.0

**Reference** <http://www.securityfocus.com/cgi-bin/vulns-item.pl?section=info&id=3294>

### Problem

- ShopPlus Cart does not filter certain types of user-supplied input from web request. This makes it possible for a malicious user to submit a request which causes arbitrary commands to be executed on the host (with the privileges of the webserver process).
- Some examples of the type of input that is not filtered:
  - host/scripts/shopplus.cgi?dn=domainname.com&cartid=%CARTID%&file=;uid|
  - host/scripts/shopplus.cgi?dn=domainname.com&cartid=%CARTID%&file=;cat%20/etc/passwd|
- Sensitive data may be disclosed to a remote attacker as a result of this issue, potentially allowing the attacker to gain local access to the host. The remote attacker will also be able to bypass authentication for the ShopPlus Cart service and access other accounts and restricted information.

### SAFER

- We are not aware of any solutions for this issue.

---

## Multiple IDS Vendor Encoded IIS Attack Detection Evasion Vulnerability

---

**Released** September 05, 2001

**Affects** Multiple IDS Products

**Reference** <http://www.securityfocus.com/cgi-bin/vulns-item.pl?section=info&id=3292>

### Problem

- Many intrusion detection systems attempt to detect attack signatures in network traffic. Web requests can be encoded, possibly obfuscating any present attack signatures. Intrusion detection systems must decode encoded traffic in order to detect attacks.
- Microsoft IIS web server supports a non-standard method of encoding web requests. Because this method is non-standard, network intrusion detection systems may not detect attacks encoded using this method.
- The method, known as '%u' encoding, involves preceding unicode bytes with the '%u' character sequence.
- An attacker may be able to send attacks (such as buffer overflows, CGI input validation attacks, etc) encoded using '%u' encoding to a target IIS webserver. While IIS will translate the encoded request, affected intrusion detection systems will not. If a signature exists for the encoded attack, it would not be detected by the IDS system.
- This vulnerability only affects intrusion detection systems in environments where '%u' unicode encoding is supported by a webserver (i.e., IIS). If there is no webserver support for this encoding method or if it is disabled, there will be no targets to which encoded attacks can be sent.
- **\*\*NOTE\*\***: Only RealSecure, Dragon IDS and Snort are confirmed vulnerable. BlackICE products detect '%u' encoded requests as being invalid, but do not decode them and detect encoded attack signatures.
- It is highly likely that IDS systems from other vendors are vulnerable as well, however this is unconfirmed. The systems we believe may be vulnerable are listed so that all possibly affected subscribers become aware of this issue.

### SAFER

- Affected vendors have released patches and updates for this vulnerability.

---

## Gauntlet Firewall for Unix and WebShield CSMAP and smap/smapi Buffer Overflow Vuln.

---

**Released** September 04, 2001

**Affects** PGP e-pliance 300 (1.0, 1.5, 2.0), Gauntlet FW Unix 5.0, 5.5, 6.0, FW 4.2

**Reference** <http://www.securityfocus.com/cgi-bin/vulns-item.pl?section=info&id=3290>

### Problem

- boundary condition error exists in the smap/smapi and CSMAPD daemons, shipped with several popular Network Associates products. The smap/smapi and CSMAP daemons are proxy servers used to handle e-mail transactions for both inbound and outbound e-mail.
- By successfully exploiting this condition, an attacker may be able to cause arbitrary code/commands to be executed on a vulnerable system with the privileges of the attacked daemon.
- Additional technical details are currently unknown.

### SAFER

- A patch to repair this vulnerability is available for all Network Associates products listed as being vulnerable.

---

## HP-UX login btmp Logging Failure Vulnerability

---

**Released** September 04, 2001

**Affects** HP-UX 10.26

**Reference** <http://www.securityfocus.com/cgi-bin/vulns-item.pl?section=info&id=3289>

### Problem

- The version of 'login' shipped with HP-UX 10.26 does not record unsuccessful login attempts in 'btmp'. The btmp file is used to record bad logins.
- It may be possible for attackers to launch a brute force attack that is not noticed by administrators who rely on btmp. As unsuccessful logins would not be recorded in the file, administrators using 'lastb' to view recent bad login attempts would not notice the attacker's attempts.
- The attempts may still be visible in other logs (such as syslog).

### SAFER

- HP has released a patch.

---

## Vibechild Directory Manager Command Execution Vulnerability

---

**Released** September 04, 2001

**Affects** Vibechild Directory Manager 0.9

**Reference** <http://www.securityfocus.com/cgi-bin/vulns-item.pl?section=info&id=3288>

### Problem

- An input validation error exists in Directory Manager that may enable remote attackers to execute arbitrary code on a host running the software. The flaw is due to a script in the package that fails to filter shell metacharacters from a user-supplied value passed to PHP's passthru() function.
- Successful exploitation of this issue is achievable by submitting shell metacharacters followed by a command in the 'userfile\_name' field of a HTTP request.
- Exploitation of this vulnerability may lead to the disclosure of sensitive data on or compromise of a vulnerable host.

### SAFER

- We are not aware of any solutions for this issue.

---

## Informix SQL SNMPDM Predictable Temporary File Creation Vulnerability

---

**Released** September 04, 2001

**Affects** IBM Informix SQL 7.31.UC5

**Reference** <http://www.securityfocus.com/cgi-bin/vulns-item.pl?section=info&id=3287>

### Problem

- A problem with the Informix SQL database add-on package makes it possible for a local user to exploit a symbolic link problem. This problem is in the snmpdm package.
- Upon execution of the setuid root application snmpdm, a file is created in the /tmp directory using filename snmpd.log. This file is created with world-writable permissions.
- Since the snmpdm program is setuid root, this makes it possible for a user to create a symbolic link in place of the snmpd.log file, and point the symbolic link to any file, existing or non-existing.
- In the case of an existing file, this allows the attacker to overwrite the file, leaving the file with permissions of 0666. If the file does not exist, a file will be created at the end of the symbolic link with permissions 0666.
- This problem could result in a local user denying service to legitimate users of the system, or potentially gaining local root access.

### SAFER

- We are not aware of any solutions for this issue.

---

## Inter7 vpopmail MySQL Authentication Data Recovery Vulnerability

---

**Released** September 04, 2001

**Affects** vpopmail (vchkw) 3.4.1 up to 4.9.10

**Reference** <http://www.securityfocus.com/cgi-bin/vulns-item.pl?section=info&id=3284>

### Problem

- A vulnerability exists in vpopmail that may result in the disclosure of sensitive authentication information when the package is configured to use a MySQL database. When the package is compiled, account information used for database authentication is compiled into an object archive and subsequently linked against the command-line programs included in the package. Due to the non-interactive nature of the package, this information is written in cleartext.
- The programs are then installed with world-readable file access permissions. As a result, it may be possible for an attacker with local access to retrieve the authentication information by examining one of the programs.

### SAFER

- We are not aware of any solutions for this issue.

---

## Informix SQL ONSRVAPD Predictable Temporary File Creation Vulnerability

---

**Released** September 04, 2001

**Affects** IBM Informix SQL 9.20.UC2 and 7.31.UC5

**Reference** <http://www.securityfocus.com/cgi-bin/vulns-item.pl?section=info&id=3283>

### Problem

- A problem in the Informix SQL package makes it possible for a local user to overwrite root-owned files, and potentially gain elevated privileges.
- The problem is in the onsvapd program. Upon execution, the program creates the predictable files onsvapd.log (owned and group member informix), and onsnmp.\$HOSTNAME.log (owned by root, group member informix) in the /tmp directory, where \$HOSTNAME is the name of Informix SQL host. The log files are created with world-writable permissions.
- Since the onsvapd program is setuid root, this makes it possible for a user to create a symbolic link in place of the onsnmp.\$HOSTNAME.log file, and point the symbolic link to any file, existing or non-existing.
- In the case of an existing file, this allows the attacker to overwrite the file, leaving the file with permissions of 0666. If the file does not exist, a file will be created at the end of the symbolic link with permissions 0666.
- This problem could result in a local user denying service to legitimate users of the system, or potentially gaining local root access.

### SAFER

- We are not aware of any solutions for this issue.

---

## FreeBSD rmuser Password Hash Disclosure Vulnerability

---

**Released** September 04, 2001

**Affects** FreeBSD 4.2 and 4.3

**Reference** <http://www.securityfocus.com/cgi-bin/vulns-item.pl?section=info&id=3282>

### Problem

- When rmuser is run, the 'passwd' and 'master.passwd' files must be updated. The rmuser script creates copies of these files and then modifies them. When complete, the original files are replaced with the updated copies.
- The script explicitly sets an insecure umask and the copy files are created world readable. If an attacker can anticipate the use of rmuser by an administrator, it may be possible to obtain the contents of 'master.passwd'. If successful, the attacker would obtain the password hashes of other users on the system. This information may assist in a brute-force password attack.
- Exploitation of this vulnerability is extremely time dependent, as the attack must be launched when rmuser is being used and while the world-readable copy exists (it is deleted by the script after the original files are overwritten).
- Attacks against this utility may be more feasible on systems where 'rmuser' is run automatically at scheduled times (for example, on a server where an automated script runs that removes ISP users with expired accounts).

### SAFER

- FreeBSD has released a source code patch.

---

## Informix SQL Temporary Log File Symbolic Link Vulnerability

---

**Released** September 04, 2001

**Affects** IBM Informix SQL 7.31.UC5

**Reference** <http://www.securityfocus.com/cgi-bin/vulns-item.pl?section=info&id=3281>

### Problem

- A problem with Informix makes it possible for local users to overwrite files, resulting in file corruption, and potentially in privilege elevation.
- The problem is due to the creation of predictable temporary files. When either the onbar\_d, ondblog, or onsmsync programs are executed, files serving as temporary logs of activity are created in /tmp. These three programs are installed with the default permissions of setuid root, and setgid informix.
- The execution of one of these three programs results in the creation of the files bar\_act.log and bar\_dbug.log in the /tmp directory. This vulnerability may be exploited only if these files do not exist or the attacker is in the informix group, as they're created with permissions 660, and cannot be removed by a user that either isn't root, or in the group informix.
- Successful exploitation of this vulnerability could lead to a denial of service, or potentially an elevation of privileges to root, although the latter is unproven.

### SAFER

- A temporary workaround is to remove the setuid and setgid bits from the affected programs. We are not aware of any vendor-supplied solutions for this issue.

---

## PGP Invalid Key Display Vulnerability

---

**Released** September 04, 2001

**Affects** PGP 5.0, 6.0.2 7.0.3, E-Business Server 6.5.8 up to 7.1, Corporate Desktop 7.1

**Reference** <http://www.securityfocus.com/cgi-bin/vulns-item.pl?section=info&id=3280>

### Problem

- When there are two user ID's on the same key, PGP's display heuristically communicates key validity to the user. The first strategy is to base the validity display on the first user ID in the key. The second is to base the validity display on the most valid key.
- The key verification window's name field uses the first strategy, while the validity light on this display uses the second strategy. Thus, when a key having an invalid user ID as the primary name and a valid user ID as the secondary name is displayed, it shows the primary user's name, but the validity of the secondary name.
- If such a key is sent to a user who relies on the affected validity displays, the key may appear to be valid. If the key is imported into the target user's keyring, attackers can forge signatures on documents sent to the target user as the invalid user-id.

### SAFER

- PGP Security has released hotfixes to address this vulnerability.

---

## HP-UX SWVerify Buffer Overflow Vulnerability

---

**Released** September 03, 2001

**Affects** HP-UX 11.0

**Reference** <http://www.securityfocus.com/cgi-bin/vulns-item.pl?section=info&id=3279>

### Problem

- A problem has been discovered in HP-UX that could allow a local user to gain elevated privileges. The vulnerability could result in complete system compromise.
- The problem is due to a buffer overflow in swverify. By supplying a string of 6039 bytes, a buffer overflow occurs, allowing the user to overwrite stack variables, including the return address.
- As the swverify program is setuid root, this makes it possible for the local user to gain an elevation of privileges to root.

### SAFER

- We are not aware of any solutions for this issue.

---

## POP3Lite Input Validation Vulnerability

---

**Released** September 03, 2001

**Affects** POP3Lite 0.2.3 and 0.2.3b

**Reference** <http://www.securityfocus.com/cgi-bin/vulns-item.pl?section=info&id=3278>

### Problem

- POP3Lite has an input validation problem which may be exploited by remote attackers. POP3Lite will not escape leading dots('.') from e-mail it transfers. POP3Lite will send lines with leading dots to the mail client, causing them to be interpreted as an end-of-message. At the very least this may cause unusual behavior to occur, but may be manipulated to malicious effect.
- For example, a message may be crafted by the attacker to a victim receiving mail from POP3Lite which causes the victim's client to accept a fake end-of-message followed by falsified arbitrary server responses. Remote attackers may exploit this issue to inject messages or cause messages to be lost. A potential for mail-spoofing attacks also exists as message headers can be falsified.
- A denial of services may also result, depending on how the client interprets the malicious input. This issue may also be exploited in combination with input validation vulnerabilities that exist in mail clients.

### SAFER

- The vendor has addressed this issue in version 0.2.4.

# SECURITY ADVISORIES

*This section contains official advisories as released by various vendors or security organizations. This list addresses the problems found during September 2001.*

---

## Conectiva Announcement CLA-2001:427: mod\_auth\_pgsql

---

**Released** September 28, 2001

**Affects** Conectiva Linux 4.1, 4.2, 5.0, e-commerce and graphic tools, 5.1, 6.0, 7.0

**Reference** <http://distro.conectiva.com.br/atualizacoes/>

### Problem

- "mod\_auth\_mysql" is an authentication module for apache which authenticates users against a PostgreSQL database. RUS-CERT discovered a vulnerability[1][3] in several Apache authentication modules which use SQL databases to retrieve user information. This vulnerability allows a remote attacker to change the query that the module sends to the SQL server and circumvent the authentication process. This vulnerability is \*still\* present in the 0.9.6 version in a slightly different fashion: Username: ";; select "bla Password: bla
- The author has been notified and released version 0.9.9 on Sep 25th to address this problem[2]. Additionally, this is also a bugfix update for this package, which wasn't linked against the PostgreSQL libraries in our previous releases.

### SAFER

- It is recommended that all mod\_auth\_pgsql users upgrade the package. All versions released here, even being older, have patches to address this problem. The update for the 0.8 version also contains the sprintf() patches from Erik Rossen.

---

## Caldera Security Advisory CSSA-2001-SCO.20: buffer overflow in BSD line printer daemon

---

**Released** September 26, 2001

**Affects** OpenServer versions lower than 5.0.6

**Reference** <http://www.calderasystems.com/support/security/>

### Problem

- The BSD-derived lpd daemon is vulnerable to a buffer overflow. This could be used by an unauthorized user to gain privilege.

### SAFER

- The proper solution is to upgrade to the latest packages.

---

## Microsoft Security Bulletin (MS01-049)

---

**Released** September 26, 2001

**Affects** Microsoft Exchange 2000 Server Outlook Web Access

**Reference** <http://www.microsoft.com/technet/security/bulletin/MS01-049.asp>

### Problem

- A security vulnerability exists in Exchange 2000 Outlook Web Access, because it will accept and process a request for an item in an authenticated user's mailbox without verifying first that the folder structure is valid. An attacker could mount a denial of service attack by repeatedly levying a request for a non-existent but deeply nested folder in his own mailbox.
- Exploiting the vulnerability wouldn't necessarily affect the OWA server itself. The effect of the vulnerability would be to cause the process servicing the attacker's mailbox to consume most or all of the CPU availability on the server it was running on. In many cases, this process would run on the OWA server, and thus the effects would be seen there. However, if the process servicing the attacker's mailbox ran on a back-end server, the effect of exploiting the vulnerability would be seen there. In any event, the affected server would resume normal service once the request was handled.

### SAFER

- Microsoft tested Exchange 5.5 and Exchange 2000 to assess whether they are affected by these vulnerabilities. Previous versions are no longer supported, and may or may not be affected by these vulnerabilities. Microsoft has released patches for this vulnerability.

---

**Cisco Security Advisory: Cisco Secure PIX Firewall SMTP Filtering Vulnerability**

---

**Released** September 26, 2001

**Affects** Cisco Secure PIX Firewalls 6.0(1), 5.2(5) and 5.2(4)

**Reference** <http://www.cisco.com/warp/public/707/SSL-J-pub.html>

**Problem**

- A security vulnerability has been discovered in version 3.x of the RSA BSAFE SSL-J Software Developer Kit made by RSA Security. This vulnerability enables an attacker to establish a Secure Socket Layer (SSL) session with the server, bypassing the client authentication and using a bogus client certificate. The server must have been developed using a vulnerable RSA BSAFE SSL-J Software Development Kit (SDK). Servers based on other libraries are not known to be vulnerable to this issue.

**SAFER**

- iCDN 2.0.1 has fixed this vulnerability. It is based on a patched RSA BSAFE SSL-J SDK provided by RSA Security.

---

**Conectiva Announcement CLA-2001:426: squid**

---

**Released** September 26, 2001

**Affects** Conectiva Linux 4.1, 4.2, 5.0, e-commerce and graphic tools, 5.1, 6.0, 7.0

**Reference** <http://distro.conectiva.com.br/atualizacoes/>

**Problem**

- Squid is a caching/proxy daemon for HTTP/FTP/Gopher. This update fixes two vulnerabilities:
- Vladimir Ivaschenko found a bug[1] which allows a remote attacker to cause a DoS on the squid proxy service by sending mkdir ftp requests.
- Takashi Taniguchi found a bug[2] that allows malicious users to do port scanning and other suspect activities using the proxy when it's configured in "http accelerator mode".
- Also, this update improves the squid script service handling (start/stop/restart/reload) and removes the suid bit from the PAM squid auth module on CL 7.0.
- Note: Conectiva Linux 7.0 is not affected by bug #2.

**SAFER**

- It is recommended that all squid users upgrade to the latest packages. This update will automatically restart the service if it is already running.

---

**Linux-Mandrake Security Update MDKA-2001:015: lyx**

---

**Released** September 25, 2001

**Affects** Mandrake Linux 8.0 (PPC)

**Reference** <http://www.linux-mandrake.com/>

**Problem**

- The LyX package would segfault under Mandrake Linux 8.0 for PPC. This update fixes the problem.

**SAFER**

---

**Update is available from Mandrake. Debian Security Advisory DSA-079-1: uucp**

---

**Released** September 24, 2001

**Affects** Debian Linux 2.2

**Reference** <http://www.debian.org/security/>

**Problem**

- zen-parse has found a problem with Taylor UUCP as distributed with many GNU/Linux distributions. It was possible to make `uux' execute `uucp' with malicious commandline arguments which gives an attacker access to files owned by uid/gid uucp.

**SAFER**

- This problem has been fixed in version of 1.06.1-11potato1 for Debian GNU/Linux 2.2 by using a patch that RedHat has provided. We recommend that you upgrade your uucp package immediately.

---

## HP Security Bulletin #0167: Vulnerability in cu(1)

---

**Released** September 24, 2001

**Affects** HP-UX 11.11, 11.00, 11.04, 10.20, 10.10, and 10.01

**Reference** <http://www.hp.com/>

### Problem

- Hewlett-Packard Company has become aware of a defect in the cu(1) command, typically used for host-to-host communication. The cu(1) command has a buffer overflow problem. By exploiting this vulnerability users could cause a denial of service (DoS).

### SAFER

- The problem can be fully resolved by applying the appropriate patches to the system.

---

## Debian Security Advisory DSA-078-1: slrn

---

**Released** September 24, 2001

**Affects** Debian Linux 2.2

**Reference** <http://www.debian.org/security/>

### Problem

- Byrial Jensen found a nasty problem in slrn (a threaded news reader). The notice on slrn-announce describes it as follows: When trying to decode binaries, the built-in code executes any shell scripts the article might contain, apparently assuming they would be some kind of self-extracting archive.

### SAFER

- This problem has been fixed in version 0.9.6.2-9potato2 by removing this feature., and we recommend that you upgrade your package immediately.

---

## FreeBSD Security Advisory SA-01:60: procmail

---

**Released** September 24, 2001

**Affects** FreeBSD + procmail

**Reference** <http://www.freebsd.org/>

### Problem

- procmail versions prior to procmail 3.20 performed unsafe actions while in the signal handlers. If a signal is delivered while procmail is already in an unsafe signal handler, undefined behaviour may result, possibly leading to the ability to perform actions as the superuser under unprivileged local user control.
- Because procmail runs setuid root, a local attacker may be able to take advantage of these problems in order to obtain superuser privileges, although there are no known exploits as of the date of this advisory.

### SAFER

- Upgrade your entire ports collection and rebuild the procmail port.

---

## Debian Security Advisory DSA-077-1: squid

---

**Released** September 24, 2001

**Affects** Debian Linux 2.2

**Reference** <http://www.debian.org/security/>

### Problem

- Vladimir Ivaschenko found a problem in squid (a popular proxy cache). He discovered that there was a flaw in the code to handle FTP PUT commands: when a mkdir-only request was done squid would detect an internal error and exit. Since squid is configured to restart itself on problems this is not a big problem.

### SAFER

- This has been fixed in version 2.2.5-3.2. This problem is logged as bug 233 in the squid bugtracker and will also be fixed in future squid releases, and we recommend that you upgrade your squid package immediately.

---

**Caldera Security Advisory CSSA-2001-SCO.19: xlock buffer overflow**

---

**Released** September 21, 2001

**Affects** UnixWare 2 version 2.1.3

**Reference** <http://www.calderasystems.com/support/security/>

**Problem**

- Very long arguments to the /usr/X/bin/xlock command would overflow an internal buffer. This could be used by a malicious user to gain privilege.

**SAFER**

- The proper solution is to upgrade to the latest packages.

---

**Linux-Mandrake Security Update MDKSA-2001:078: uucp**

---

**Released** September 21, 2001

**Affects** Mandrake Linux 7.1, 7.2, 8.0 and CS 1.0.1

**Reference** <http://www.linux-mandrake.com/>

**Problem**

- Zen Parse discovered that an argument-handling problem that exists in the uucp package could allow a local attacker to gain access to the uucp user or group.

**SAFER**

- Update is available from Mandrake.

---

**Caldera Security Advisory CSSA-2001-SCO.18: su buffer overflow**

---

**Released** September 21, 2001

**Affects** UnixWare 2 version 2.1.3

**Reference** <http://www.calderasystems.com/support/security/>

**Problem**

- The /usr/bin/su command was vulnerable to several buffer overflows that could be exploited by a malicious user.

**SAFER**

- The proper solution is to upgrade to the latest packages.

---

**SuSE Security Announcement SuSE-SA:2001:032: wmaker/WindowMaker**

---

**Released** September 20, 2001

**Affects** SuSE Linux (6.0, 6.1, 6.2), 6.3, 6.4, 7.0, 7.1 and 7.2

**Reference** <http://www.suse.com/>

**Problem**

- The window manager Window Maker was found vulnerable to a buffer overflow due to improper bounds checking when setting the window title. An attacker can remotely exploit this buffer overflow by using malicious web page titles or terminal escape sequences to set an excessively long window title.
- This attack can lead to remote command execution with the privileges of the user running Window Maker.

**SAFER**

- Update package is available from SuSE.

---

**Caldera Security Advisory CSSA-2001-SCO.17: vi /tmp vulnerability**

---

**Released** September 19, 2001

**Affects** OpenServer all versions

**Reference** <http://www.calderasystems.com/support/security/>

**Problem**

- The vi editor uses temporary names that are predictable. A user could use this vulnerability to write arbitrary files.

**SAFER**

- The proper solution is to upgrade to the latest packages.

---

**Red Hat Security Advisory RHSA-2001:110-05: initscript**

---

**Released** September 19, 2001

**Affects** Red Hat Linux

**Reference** <http://www.redhat.com/>

**Problem**

- The setserial package comes with an initscript in the documentation directory. If this initscript is manually copied into the init.d directory structure and enabled, and the kernel is recompiled to have modular serial port support, then the initscript will use a predictable temporary file name.
- There are a number of other bugs that also prevent the initscript from working correctly in this situation (detailed in bugzilla bug #52862).

**SAFER**

- Do not use the initscript supplied with setserial. To disable it, use the following command: `/sbin/chkconfig serial off`. Alternatively, if your system needs manual adjustment of its serial port settings and you wish to have those adjustments re-applied automatically on boot, be sure to use a kernel that has non-modular serial port support, such as those supplied by Red Hat.

---

**Debian Security Advisory DSA-076-1: most**

---

**Released** September 18, 2001

**Affects** Debian Linux 2.2

**Reference** <http://www.debian.org/security/>

**Problem**

- Pavel Macek has found a buffer overflow in the `most' pager program. The problem is part of most's tab expansion where the program would write beyond the bounds of two array variables when viewing a malicious file. This could lead into other data structures being overwritten which in turn could enable most to execute arbitrary code being able to compromise the users environment.

**SAFER**

- This has been fixed in the upstream version 4.9.2 and an updated version of 4.9.0 for Debian GNU/Linux 2.2, and we recommend that you upgrade your most package immediately.

---

**Caldera Security Advisory CSSA-2001-SCO.16: lp utility commands**

---

**Released** September 18, 2001

**Affects** UnixWare 7 and Open Unix

**Reference** <http://www.calderasystems.com/support/security/>

**Problem**

- Very long arguments to the line printer utilities accept, reject, enable and disable caused a segmentation violation. This could be used by an unauthorized user to gain privilege.

**SAFER**

- The proper solution is to upgrade to the latest packages.

---

## Linux-Mandrake Security Update MDKSA-2001:077: apache

---

**Released** September 18, 2001

**Affects** Mandrake Linux 7.1, 7.2, 8.0 and CS 1.0.1

**Reference** <http://www.linux-mandrake.com/>

### Problem

- A problem exists with all Apache servers prior to version 1.3.19. The vulnerability could allow directory indexing and path discovery on the vulnerable servers with a custom crafted request consisting of a long path name created artificially by using numerous slashes. This can cause modules to misbehave and return a listing of the directory contents by avoiding the error page.
- Because of the number of add-on packages Mandrake Linux provides for Apache that are compiled for a specific version of Apache, and due to the complexity of the upgrade, we recommend that users upgrade Apache and all associated packages by hand, invoking RPM directly. The updates provide updated Apache, PHP, mod\_perl, and mod\_ssl packages for all relevant versions, and all should be upgraded at the same time to avoid dependency issues. You can do this by using the "rpm -Fvh \*.rpm" command from a temporary directory containing the relevant update packages.
- Due to a packaging error in previous versions of mod\_php3 for Linux- Mandrake 7.1, you will need to manually edit /etc/httpd.conf to re- enable PHP support. You can do this by issuing, as root: echo "Include conf/addon-modules/php.conf" >>/etc/httpd/conf/httpd.conf.
- Additionally, we have updated PHP to version 4.0.6 for Mandrake Linux 8.0.

### SAFER

- Update is available from Mandrake.

---

## Cisco Security Advisory: Vulnerable SSL implementation in iCDN

---

**Released** September 12, 2001

**Affects** Cisco iCDN 2.0

**Reference** <http://www.cisco.com/warp/public/707/PIXfirewallSMTPfilter-regression-pub.shtml>

### Problem

- The Cisco Secure PIX firewall feature "mailguard" which limits SMTP commands to a specified minimum set of commands can be bypassed. This vulnerability can be exploited to bypass SMTP command filtering.
- If the mail server itself is not properly secured, an attacker may be able to collect information about existing e-mail accounts and aliases, or may be able to execute arbitrary code on the mail server. In order to exploit this vulnerability, an attacker would need to also exploit the mailserver that is currently protected by the PIX. If that server is already well configured, and has the latest security patches and fixes from the SMTP vendor, that will minimize the potential for exploitation of this vulnerability.

### SAFER

- Fixes are available from Cisco.

---

## Linux-Mandrake Security Update MDKSA-2001:073-1: xli/xloadimage

---

**Released** September 12, 2001

**Affects** Mandrake Linux 7.1, 7.2, 8.0 and CS 1.0.1

**Reference** <http://www.linux-mandrake.com/>

### Problem

- A buffer overflow exists in xli due to missing boundary checks. This could be triggered by an external attacker to execute commands on the victim's machine. An exploit is publicly available. xli is an image viewer that is used by Netscape's plugger to display TIFF, PNG, and Sun-Raster images.

### SAFER

- The xloadimage package uses the same code as xli and is likewise vulnerable. An update is provided for xloadimage which was only provided with Linux-Mandrake 7.2.

---

**Conectiva Announcement CLA-2001:425: uucp**

---

**Released** September 11, 2001

**Affects** Conectiva Linux 4.1, 4.2, 5.0, e-commerce and graphic tools, 5.1, 6.0, 7.0

**Reference** <http://distro.conectiva.com.br/atualizacoes/>

**Problem**

- UUCP is a Unix-to-Unix transfer mechanism. It is used primarily for remote sites to download and upload email and news files to local machines. zen-parse found[1] a vulnerability in the command-line argument handling of uucp which can be exploited by a local user to obtain uid/gid uucp.

**SAFER**

- All users with the uucp package installed should upgrade.

---

**HP Security Bulletin #0145: Vulnerability in asecur (Rev.03)**

---

**Released** September 10, 2001

**Affects** HP-UX 10.01, 10.10, 10.20 and 11.00

**Reference** <http://www.hp.com/>

**Problem**

- Certain files used by the asecur program have unsafe permissions. This problem can lead to possible denial of service.

**SAFER**

- Install the appropriate patch.

---

**SuSE Security Announcement SuSE-SA:2001:31: apache-contrib**

---

**Released** September 10, 2001

**Affects** SuSE Linux 7.1 and 7.2

**Reference** <http://www.suse.com/>

**Problem**

- The Apache module mod\_auth\_mysql 1.4, which is shipped since SuSE Linux 7.1, was found vulnerable to possible bypass authentication by MySQL command injection. An adversary could insert MySQL commands along with a password and these commands will be interpreted by MySQL while mod\_auth\_mysql is doing the password lookup in the database. A positive authentication could be returned.
- Note, that this bug has not yet been proven exploitable so far.

**SAFER**

- Update package is available from SuSE.

---

**Red Hat Security Advisory RHSA-2001:107-07: bugzilla**

---

**Released** September 10, 2001

**Affects** Red Hat Powertools 7.0 and 7.1

**Reference** <http://www.redhat.com/>

**Problem**

- Bugzilla-2.14 is a general security update. The serious security problems fixed are: multiple instances where valid users could obtain data on "confidential" bugs without authorization, multiple instances of security holes where parameters were not being checked/escaped properly.

**SAFER**

- Updates are available from RedHat. It is recommended that all users update to the fixed packages.

---

**Microsoft Security Bulletin (MS01-048)**

---

**Released** September 10, 2001

**Affects** Microsoft Windows NT4

**Reference** <http://www.microsoft.com/technet/security/bulletin/MS01-048.asp>

**Problem**

- The RPC endpoint mapper allows RPC clients to determine the port number currently assigned to a particular RPC service. The Windows NT 4.0 endpoint mapper contains a flaw that causes it to fail upon receipt of a request that contains a particular type of malformed data.
- Because the endpoint mapper runs within the RPC service itself, exploiting this vulnerability would cause the RPC service itself to fail, with the attendant loss of any RPC-based services the server offers, as well as potential loss of some COM functions. Normal service could be restored by rebooting the server.

**SAFER**

- Microsoft has released patches for this vulnerability.

---

**NetBSD Security Advisory 2001-017: sendmail(8) incorrect command line argument check**

---

**Released** September 07, 2001

**Affects** NetBSD 1.5, 1.5.1 and CURRENT

**Reference** <http://www.netbsd.org/Security/>

**Problem**

- Certain variables were treated as signed values, but should have been unsigned. Bounds checking was not done when incrementing an index. Combined with supplied command-line arguments, a local user could exploit the setuid-root sendmail binary and the lack of bounds checking to perform a root compromise.

**SAFER**

- Upgrade to sendmail 8.11.6.

---

**Caldera Security Advisory CSSA-2001-033.0: Linux - uucp argument handling problems**

---

**Released** September 07, 2001

**Affects** Caldera OpenLinux 2.3, eServer 2.3.1, eDesktop 2.4, Server 3.1, Workstation 3.1

**Reference** <http://www.calderasystems.com/support/security/>

**Problem**

- There is an argument-handling problem which allows a local attacker to gain access to the uucp group. Using this access the attacker could use badly written scripts to gain access to the root account.

**SAFER**

- The proper solution is to upgrade to the latest packages.

---

**NetBSD Security Advisory 2001-016: unsafe chdir usage in fts(3)**

---

**Released** September 07, 2001

**Affects** All NetBSD releases

**Reference** <http://www.netbsd.org/Security/>

**Problem**

- The macro for chdir used in libc/gen/fts (\_\_fts13.c after NetBSD 1.3) did not perform sufficient safety checks. If any directory (or symlink to a directory) above the current directory fts was processing was moved, the fts-using application could be made to descend the wrong directory sub-tree, and/or ascend above the original starting directory. Once it has ascended above the starting directory, the process could descend into an unintended file system hierarchy.
- This is particularly dangerous when combined with automated scripts which run programs such as 'rm -r'.

**SAFER**

- Patches are available from NetBSD.

---

**Red Hat Security Advisory RHSA-2001:109-05: xinetd**

---

**Released** September 07, 2001

**Affects** Red Hat Linux 7.0 and 7.1

**Reference** <http://www.redhat.com/>

**Problem**

- A security audit has been done by Solar Designer on xinetd, and the results are now being made available as a preemptive measure. Also, memsetting too much memory to 0 would eventually lead to segfaults when executing services. This internal bug was fixed.

**SAFER**

- Updates are available from RedHat. It is recommended that all users update to the fixed packages.

---

**IBM MSS Advisory MSS-OAR-E01-2001:391.1: Buffer Overflow Vulnerabilities in lpd**

---

**Released** September 07, 2001

**Affects** AIX 4.3.x and 5.1

**Reference** <http://www-1.ibm.com/services/brs/brspwhub.nsf/advisories/>

**Problem**

- The Line Printer daemon, lpd, shipped with AIX contains several buffer overflow vulnerabilities that potentially allow a malicious remote user to gain root privileges. Two of the three vulnerabilities found require the attacker's system be listed in /etc/hosts.lpd or /etc/hosts.equiv. The third requires that the malicious user have control over the victim's domain name server (DNS).
- A malicious local or remote user can use a well-crafted exploit code to gain root privileges on the attacked system, compromising the integrity of the system and its attached local network. If the malicious user is unable to gain root access, he or she could still cause a system crash (DoS) via this vulnerability.
- 

**SAFER**

- Temporary fixes for AIX 4.3.x and 5.1 systems are available. IBM is working on the full fixes which will be available soon.

---

**FreeBSD Security Advisory SA-01:57: sendmail (REVISED)**

---

**Released** September 06, 2001

**Affects** FreeBSD 4.1.1-RELEASE, 4.2-RELEASE, 4.3-RELEASE and 4-STABLE

**Reference** <http://www.freebsd.org/>

**Problem**

- Sendmail contains an input validation error which may lead to the execution of arbitrary code with elevated privileges by local users. Due to the improper use of signed integers in code responsible for the processing of debugging arguments, a local user may be able to supply the signed integer equivalent of a negative value supplied to sendmail's "trace vector". This may allow a local user to write data anywhere within a certain range of locations in process memory. Because the '-d' command-line switch is processed before the program drops its elevated privileges, the attacker may be able to cause arbitrary code to be executed with root privileges.

**SAFER**

- Upgrade your vulnerable FreeBSD system to 4.3-STABLE or the RELENG\_4\_3 security branch after the respective correction dates.

---

**Red Hat Security Advisory RHSA-2001:106-06: sendmail**

---

**Released** September 06, 2001

**Affects** Red Hat Linux 5.2, 6.2, 7.0 and 7.1

**Reference** <http://www.redhat.com/>

**Problem**

- Sendmail, the low-level system for sending and receiving email for Red Hat Linux, has an input validation flaw in part of its debugging code. This flaw could be exploited by an attacker who already has local access to a system and wants to gain root privileges. Red Hat is issuing new sendmail packages that correct this flaw for all our currently supported Red Hat Linux platforms.

**SAFER**

- Updates are available from RedHat. All users are strongly advised to apply these fixes.

---

**NetBSD Security Advisory 2001-015: Insufficient checking of lengths passed to kernel**

---

**Released** September 06, 2001

**Affects** NetBSD 1.4, 1.5, 1.5.1 and CURRENT

**Reference** <http://www.netbsd.org/Security/>

**Problem**

- The problem for which NetBSD SA2001-011 was issued ("Insufficient msg\_controllen checking for sendmsg(2)") urged an audit of NetBSD code to look for similar issues in other parts of kernel. A number of issues were found. In a number of places lengths or sizes passed from userland were used by the kernel without sufficient checks. Most of the problems involved errors handling signed versus unsigned values, in some cases the code was not checking for negative values. The actual severity of these problems varies, and three different problem severity groups have been identified:
  - semop(2) - exploitable by any user for denial of service or to execute arbitrary kernel code.
  - mount args - exploitable by any user for denial of service if user mounts are enabled (it's disabled by default on NetBSD 1.5 and later).
  - some device ioctls - exploitable by any user with write access to appropriate device files (by default only root has write access on most device files).

**SAFER**

- Patches are available from NetBSD.

---

**Microsoft Security Bulletin (MS01-047)**

---

**Released** September 06, 2001

**Affects** Microsoft Exchange 5.5

**Reference** <http://www.microsoft.com/technet/security/bulletin/MS01-047.asp>

**Problem**

- Among the functions Outlook Web Access (OWA) in Exchange 5.5 offers is the ability to search the global address list (GAL). By design, this is an authenticated function, implemented as a two-tier architecture - a front tier that provides a user interface and a back-end tier that actually performs the search. However, only the front tier actually checks authentication. An attacker who sent a properly formatted request to the back-end function that actually performs the search could enumerate the GAL without authenticating.

**SAFER**

- Microsoft has released patches for this vulnerability.

---

**Red Hat Security Advisory RHSA-2001:103-04: fetchmail**

---

**Released** September 06, 2001

**Affects** Red Hat Linux 5.2, 6.2, 7.0 and 7.1

**Reference** <http://www.redhat.com/>

**Problem**

- Fetchmail versions up to 5.8.9 are susceptible to remote attacks from malicious servers. When fetchmail attempts to create an index of messages in the remote mailbox being polled, it uses index numbers sent by the server as an index into an internal array. If a server sends fetchmail a negative number, fetchmail will attempt to write data outside the bounds of the array.

**SAFER**

- Updates are available from RedHat. It is recommended that all users update to the fixed packages.

---

**Conectiva Announcement CLA-2001:421: mod\_auth\_mysql**

---

**Released** September 06, 2001

**Affects** Conectiva Linux 4.0, 4.0es, 4.1, 4.2, 5.0, e-commerce and graphic tools, 5.1, 6.0, 7.0

**Reference** <http://distro.conectiva.com.br/atualizacoes/>

**Problem**

- "mod\_auth\_mysql" is an authentication module for apache which authenticates users against a MySQL database. RUS-CERT[3] discovered a vulnerability[1][2] in several Apache authentication modules which use SQL databases to retrieve user information. This vulnerability allows a remote attacker to change the query that the module sends to the SQL server and potentially circumvent the authentication process. The mysql\_query() function, used by this module, does not allow multiple commands to be sent to the server, that is, the ";" character is not allowed. This restricts this vulnerability somewhat, since the attacker can no longer issue other commands besides the SELECT one the module is already doing, but he/she can still mangle this query and this should not be underestimated.
- Additionally, this update also fixes a problem with this package which wasn't linked against the MySQL libraries in previous releases.

**SAFER**

- All mod\_auth\_mysql users should upgrade. It is necessary to restart the apache server after applying the update.

---

**Red Hat Security Advisory RHSA-2001:072-14: man**

---

**Released** September 06, 2001

**Affects** Red Hat Linux 5.2, 6.2, 7.0 and 7.1

**Reference** <http://www.redhat.com/>

**Problem**

- Users could gain access to the GID man by overrunning a buffer in the ultimate\_source() function. Users with GID man could get root access by creating man pages with filenames containing escape characters. Furthermore, the previous errata package hardcoded Red Hat Linux 7.x man paths even on Red Hat Linux 5.x and 6.x.

**SAFER**

- Updates are available from RedHat. It is recommended that all users update to the fixed packages.

---

**HP Security Bulletin #0166: Vulnerability in libsecurity (VVOS)**

---

**Released** September 05, 2001

**Affects** HP-UX 11.04 (VVOS), VirtualVault only

**Reference** <http://www.hp.com/>

**Problem**

- Hewlett-Packard Company has discovered that a problem in libsecurity.2 causes unexpected resource handling problems. This problem can lead to possible denial of service.

**SAFER**

- The patch is available.

---

**SuSE Security Announcement SuSE-SA:2001:030: screen**

---

**Released** September 05, 2001

**Affects** SuSE Linux (6.0, 6.1, 6.2), 6.3, 6.4, 7.0, 7.1 and 7.2

**Reference** <http://www.suse.com/>

**Problem**

- screen is a terminal multiplexer program that allows reattaching to a detached session as well as multi-attached (shared) sessions. The screen package allows a local attacker to obtain root privileges if the /usr/bin/screen command is installed setuid root and if a directory below /tmp/screens/ exists.
- The screen program needs root permissions from the setuid-root bit for two reasons: multi-attached sessions are only possible with root privileges, and writing terminal allocation information to /var/run/utmp (the who(1) and finger(1) commands). If the screen command is not running with special privileges, all functionality except these two features will continue to work, but the local root compromise will not be possible. In order to provide the features mentioned, the screen package used to be installed setuid-root in SuSE Linux distributions.
- The update packages that we provide for the supported distributions 6.3, 6.4, 7.0, 7.1 and 7.2 eliminate the error in the source code. In addition to that, the rpm package does not contain the setuid-bit on the screen program any more. If there is any more security-related bug in the screen package or libraries that it is linked against to be found in the future, these errors will not open local security holes any more. Users of the screen package who need the multi-attach feature must enable it again by adding the setuid-bit to the /usr/bin/screen file. Please note that you should reflect the changes to permissions in the files /etc/permissions\*. If unsure, use the setting "secure local" for the variable PERMISSION\_SECURITY in /etc/rc.config and execute "SuSEconfig" as root. Alternatively, change the settings for the screen program in /etc/permissions\* and run "chkstat -set <file>" for each file that you need. Use the command "rpm -qlv screen | grep /usr/bin" to find out which files to add to the permissions file (/usr/bin/screen is a symlink).
- The authors of screen have released the new version screen-3.9.10 that fixes the multi-attach-error, and some other uncritical bug. Our update packages contain the necessary patches applied to the version as shipped with the original distribution.

**SAFER**

- Update package is available from SuSE.

---

**ISS Alert: Multiple Vendor IDS Unicode Bypass Vulnerability**

---

**Released** September 05, 2001

**Affects** Multiple IDS Vendors

**Reference** <http://xforce.iss.net/>

**Problem**

- Unicode provides a standard for international character sets by assigning a unique number for each character. It comprises the character repertoire of most commonly used character sets like ASCII, ANSI, ISO-8859, Cyrillic, Greek, Chinese, Japanese and Korean. Unicode encoding of ASCII characters can be used to obfuscate the appearance of an HTTP request, while leaving it functional. This allows attackers to disguise the payload used in an exploit and evade detection. The first major Unicode vulnerability was documented against Microsoft Internet Information Server (IIS) in October 2000. This vulnerability allowed attackers to encode "/", "\" and "." characters to appear as their Unicode counterparts and bypass the security mechanisms within IIS that block directory traversal.
- Unicode encoding can also be used to evade IDS detection due to a flaw in Microsoft IIS that accepts and interprets non-standard Unicode characters.

**SAFER**

- Users of affected IDS products should contact their vendor immediately to obtain a patch or workaround.

---

**Conectiva Announcement CLA-2001:420: mailman**

---

**Released** September 05, 2001

**Affects** Conectiva Linux 4.1, 4.2, 5.0, 5.1, 6.0, 7.0

**Reference** <http://distro.conectiva.com.br/atualizacoes/>

**Problem**

- Mailman is a mailing list manager. This update fixes two security problems and some other issues not related to security:
- Versions prior do 2.0.2 (affects CL<=6.0) have a vulnerability which allows a list administrator to obtain the list password of a subscriber. This is not a regular security problem because the list administrator does not need that password to gain access to a user's subscription, but it is quite possible that the user shares this password with other services, such as an email account, even though the web interface gives a clear warning about this password and how it is handled (by default, the password is mailed out every month).
- Versions prior do 2.0.6 (affects CL<=7.0) have a vulnerability which could allow non-authorized users to gain access to the administrative interface of a list. For this to happen, the global password (located in the data/adm.pw file) has to be empty, which is not very likely. If it is empty, the administrative interface will accept any password as valid.
- This update also brings a logrotate configuration file to our mailman package. This will regularly rotate the logs in /usr/lib/mailman/logs.
- Version 2.0.5 (affects CL<=7.0) fixed a problem with stale lock files which can cause a list to be inaccessible for long periods of time until the lock expires or is removed manually.

**SAFER**

- All mailman administrators should upgrade. It is recommended that the update be applied while the server is inactive, that is, the web interface should be disabled during this period as well as the MTA and crond, since many mailman processes are started at different times via cron.

---

**Cisco Security Advisory: Cisco Secure IDS Signature Obfuscation Vulnerability**

---

**Released** September 05, 2001

**Affects** Cisco Secure IDS Sensor component, Catalyst 6000 Intrusion Detection System Module

**Reference** <http://www.cisco.com/warp/public/707/cisco-intrusion-detection-obfuscation-vuln-pub.shtml>

**Problem**

- Intrusion Detection Systems inspect network traffic for suspect or malicious packet formats, data payloads and traffic patterns. Intrusion detection systems typically implement obfuscation defense - ensuring that suspect packets cannot easily be disguised with UTF and/or hex encoding and bypass the Intrusion Detection systems. Recently, the CodeRed worm has targeted an unpatched vulnerability with many MicroSoft IIS systems and also highlighted a different encoding technique supported by MicroSoft IIS systems. This encoding technique known as %u can be used to circumvent intrusion detection systems.

**SAFER**

- Cisco has corrected this vulnerability in the Cisco Secure Intrusion Detection System, formerly known as Netranger, with a service pack that is now available to customers. This vulnerability also affects the Cisco Catalyst 6000 Intrusion Detection System Module, and will be repaired in a service pack for version 3.0, which is not yet released.

---

**Conectiva Announcement CLA-2001:419: fetchmail**

---

**Released** September 05, 2001

**Affects** Conectiva Linux 4.0, 4.0es, 4.1, 4.2, 5.0, e-commerce and graphic tools, 5.1, 6.0, 7.0

**Reference** <http://distro.conectiva.com.br/atualizacoes/>

**Problem**

- Fetchmail is a program used to retrieve email from POP and IMAP servers. Salvatore Sanfilippo did an audit and found a remote vulnerability in fetchmail that allows a remote attacker to write arbitrary data into memory. To take advantage of this problem, an attacker has to have control over the mail server being queried by the fetchmail process.

**SAFER**

- All fetchmail users should upgrade. If fetchmail is running as a daemon, it will have to be restarted after applying the update in order to run the new version.

---

**FreeBSD Security Advisory SA-01:59: rmuser (REVISED)**

---

**Released** September 04, 2001

**Affects** FreeBSD 4.2-RELEASE, 4.3-RELEASE and 4.3-STABLE

**Reference** <http://www.freebsd.org/>

**Problem**

- When removing a user from the system with the rmuser utility, the /etc/master.passwd file and its corresponding database /etc/spwd.db must be updated. The rmuser script was incorrectly doing this by creating a new master.passwd file with an unsafe umask and then using chmod to set its permissions to 0600. Between the time that the file was created and the time that its permissions were changed the file is world-readable.
- This is only a minor security vulnerability since the rmuser command is only used infrequently on most systems, and the attack is highly timing-dependent.

**SAFER**

- Upgrade your vulnerable system to 4.3-STABLE or the RELENG\_4\_3 security branch, dated after the respective correction dates.

---

**SuSE Security Announcement SuSE-SA:2001:029: nkitb/nkitserv/telnetd**

---

**Released** September 03, 2001

**Affects** SuSE Linux [6.1, 6.2], 6.3, 6.4, 7.0, 7.1 and 7.2

**Reference** <http://www.suse.com/>

**Problem**

- The telnet server which is shipped with SuSE distributions contains a remotely exploitable buffer-overflow within its telnet option negotiation code. This bug is wide-spread on UN\*X systems and affects almost all implementations of telnet daemons available. SuSE 7.2 distribution ships the telnet-server package which contains the vulnerable telnet daemon. This package has been fixed.
- The SuSE Linux distributions 6.3 and 6.4 contain versions and implementations of the telnet-daemon that are vulnerable, but the complexity of the code requires a full source code audit of the software. In order not to further delay the release of the packages for the SuSE Linux 7.x distributions, we recommend to disable the telnet daemon on the 6.x distributions. This can be done by commenting out the line in /etc/inetd.conf that starts with "telnet", and then reloading the inetd configuration using the command "killall -1 inetd". Another option is to not start the inetd in the first place if you do not need any of the services provided by the inetd daemon. Disabling inetd permanently involves killing the running inetd process ("killall -TERM inetd") and setting the variable START\_INETD in /etc/rc.config to "no" (as opposed to "yes"). Disabling the telnet service is the preliminary solution/workaround against the problems with the telnetd daemon. We hope to be able to provide a better solution.
- The SuSE Linux distributions 7.0, 7.1 and 7.2 have similar implementations of in.telnetd, and for all of these distributions there are update packages available. Please note that the package that contains the /usr/sbin/in.telnetd program (the server program) has changed over the different releases of the SuSE Linux distribution. In the 7.0 and 7.1 distributions the package is called "nkitserv". The 7.2 distribution lists the telnet server in the package "telnet-server".

**SAFER**

- Please download the packages and verify them. After successful authentication you can update your packages with the command `rpm -Uhv file.rpm'. Further action should not be necessary to activate the update since the in.telnetd daemon is started from a new by inetd upon every accepted connection from the network. Regardless of the availability of fixed packages of the telnet-daemon, SuSE Security strongly recommends to disable the telnet service if you do not use it. In addition to that, only cryptographically protected protocols such as secure shell (ssh, package openssh) can be an efficient countermeasure against sniffing and spoofing type attacks. Due to significantly more comfort (such as X11-forwarding, multiple authentication methods, ...), the transition to ssh should be worth the effort in any case.

---

**Linux-Mandrake Security Update MDKSA-2001:076: xinetd**

---

**Released** September 01, 2001

**Affects** Mandrake Linux 7.2, 8.0 and SNF 7.2

**Reference** <http://www.linux-mandrake.com/>

**Problem**

- An audit has been performed on the xinetd 2.3.0 source code by Solar Designer for many different possible vulnerabilities. The 2.3.1 release incorporated his patches into the xinetd source tree. The audit was very thorough and found and fixed many problems. This xinetd update includes his audit patch.

**SAFER**

- Update is available from Mandrake.

---

**Linux-Mandrake Security Update MDKSA-2001:075: sendmail**

---

**Released** September 01, 2001

**Affects** Mandrake Linux 7.2 and 8.0

**Reference** <http://www.linux-mandrake.com/>

**Problem**

- An input validation error exists in sendmail that may allow local users to write arbitrary data to process memory. This could possibly allow the execution of code or commands with elevated privileges and may also allow a local attacker to gain access to the root account.

**SAFER**

- Update is available from Mandrake.

---

**Linux-Mandrake Security Update MDKSA-2001:074: WindowMaker**

---

**Released** September 01, 2001

**Affects** Mandrake Linux 7.1, 7.2, 8.0 and CS 1.0.1

**Reference** <http://www.linux-mandrake.com/>

**Problem**

- A buffer overflow exists in the WindowMaker window manager's window title handling code, as discovered by Alban Hertroys. Many programs, such as web browsers, set the window title to something obtained from the network, such as the title of the currently viewed web page. As such, this buffer overflow could be exploited remotely. WindowMaker versions above and including 0.65.1 are fixed upstream; these packages have been patched to correct the problem.

**SAFER**

- Update is available from Mandrake.

---

**Linux-Mandrake Security Update MDKSA-2001:073: xli**

---

**Released** September 01, 2001

**Affects** Mandrake Linux 7.1, 7.2, 8.0 and CS 1.0.1

**Reference** <http://www.linux-mandrake.com/>

**Problem**

- A buffer overflow exists in xli due to missing boundary checks. This could be triggered by an external attacker to execute commands on the victim's machine. An exploit is publicly available. xli is an image viewer that is used by Netscape's plugger to display TIFF, PNG, and Sun-Raster images.

**SAFER**

- Update is available from Mandrake.

---

**Linux-Mandrake Security Update MDKSA-2001:072: fetchmail**

---

**Released** September 01, 2001

**Affects** Mandrake Linux 7.1, 7.2, 8.0 and CS 1.0.1

**Reference** <http://www.linux-mandrake.com/>

**Problem**

- A vulnerability was found by Salvatore Sanfilippo in both the IMAP and POP3 code of fetchmail where the input is not verified and no bounds checking is done. This can be exploited by a remote attacker to write arbitrary data into memory. The attacker must have control of the mail server the client is connecting to via fetchmail in order to exploit this vulnerability.

**SAFER**

- Update is available from Mandrake.

# DENIAL-OF-SERVICE

*Denial-of-Service attacks are becoming an increasing concern. Below is a compilation of denial-of-service security problems found in September 2001.*

---

## **3Com HomeConnect Cable Modem External with USB Denial of Service Vulnerability**

---

**Released** September 26, 2001

**Affects** 3Com HomeConnect Cable Modem External with USB

**Reference** <http://www.securityfocus.com/cgi-bin/vulns-item.pl?section=info&id=3366>

### **Problem**

- A problem in the firmware running the cable modem could allow a denial of service. It is possible to reset the modem by connecting to the HTTP service and requesting a long string in the following format: `http://targetip/AAAAAA.....` where A is repeated 100 times.
- This problem makes it possible for a remote user to deny service to legitimate users of networks serviced by the modem.
- This vulnerability is most likely related to BugTraq ID 2721.
- It is possible that this behaviour is due to a buffer overflow condition. If this is the case, and the attacker is familiar with the firmware/hardware, it may be possible to force the execution of attacker-supplied instructions.

### **SAFER**

- As a workaround, users can block port 80 traffic by setting up a filter with the modem's firmware. We are not aware of any vendor-supplied solutions for this issue.

---

## **QPC Software QVT/Term FTP Denial of Service Vulnerability**

---

**Released** September 25, 2001

**Affects** QPC Software QVT/Term 5.0

**Reference** <http://www.securityfocus.com/cgi-bin/vulns-item.pl?section=info&id=3363>

### **Problem**

- A vulnerability exists in QVT's FTP daemon which could cause a denial of services. This is achieved by connecting to port 21 and submitting an unusually long string of arbitrary characters.
- Successful exploitation of this vulnerability could result in the loss of FTP services. A restart of the service may be required in order to gain normal functionality.
- This issue may be the result of an unchecked buffer. If this is the case, there is a possibility that arbitrary code may be executed on the vulnerable host. However, this has not yet been confirmed.

### **SAFER**

- We are not aware of any solutions for this issue.

---

## **Compaq TruCluster Port Scan Denial of Service Vulnerability**

---

**Released** September 25, 2001

**Affects** Compaq TruCluster 1.5

**Reference** <http://www.securityfocus.com/cgi-bin/vulns-item.pl?section=info&id=3362>

### **Problem**

- A problem has been discovered that could allow a denial of service to users of the TruCluster package. The problem is in the handling of port scans by the software.
- When a system is port scanned from a system without a DNS PTR record in DNS, the cluster develops split-brain. Split-brain is a condition that results from another server in the cluster being started to take over the operations of a failed server while there's still another system running.
- This can result in corrupted or destroyed data, denial of service, and even hardware damage.

### **SAFER**

- We are not aware of any solutions for this issue.

---

## IBM HACMP Port Scan Denial of Service Vulnerability

---

**Released** September 24, 2001

**Affects** IBM HACMP 4.4

**Reference** <http://www.securityfocus.com/cgi-bin/vulns-item.pl?section=info&id=3358>

### Problem

- A problem has been reported in the software package that could allow a denial of service to legitimate users of systems managed by the suite.
- The problem is due to the handling of port scans by HACMP clusters. When an HACMP cluster is port scanned by another system, and the ports can use the connect() function of TCP, the system in the cluster will fail. It is reported that this occurs on systems that have the HACMP ports connect() scanned, and the systems are unaffected by TCP SYN stealth scans.
- Each system within the cluster that is scanned fails. This could result in assets managed by the cluster becoming unusable, thus denying service to legitimate users of the systems.

### SAFER

- We are not aware of any solutions for this issue.

---

## Squid Web Proxy Cache Denial of Service Vulnerability

---

**Released** September 21, 2001

**Affects** Squid Web Proxy 2.3 and 2.4

**Reference** <http://www.securityfocus.com/cgi-bin/vulns-item.pl?section=info&id=3354>

### Problem

- A problem exists in the manner which Squid handles requests to make FTP directories on proxied services. A specially crafted "mkdir-only" PUT request which is passed through the Squid proxy to a remote FTP server will be sufficient to cause a denial of service to the proxy.
- For example: nc proxy:3128; PUT ftp://ftpserver/WEB-INF/1/2/1/ HTTP/1.1; Content-type: application/octet-stream; Content-length: 0; Pragma: no-cache
- If affected with a denial of service then Squid must be restarted to regain normal functionality.

### SAFER

- The vendor has released patches which address this issue.

---

## HP-UX VVOS libsecurity Denial of Service Vulnerability

---

**Released** September 13, 2001

**Affects** HP-UX (VVOS) 11.0.4

**Reference** <http://www.securityfocus.com/cgi-bin/vulns-item.pl?section=info&id=3338>

### Problem

- A library function in libsecurity contains a vulnerability that may allow for local attackers to cause a denial of service. The offending function is 'putprpwnam()', a call used to update or write new protected password file entries to the password file.
- It may be possible for attackers to exploit programs which call this function. The consequence of exploitation may be a denial of service.

### SAFER

- HP has made a fix available.

---

## EFTP Buffer Overflow Code Execution and Denial of Service Vulnerability

---

**Released** September 12, 2001

**Affects** Khamil Landross and Zack Jones EFTP 2.0.7.337

**Reference** <http://www.securityfocus.com/cgi-bin/vulns-item.pl?section=info&id=3330>

### Problem

- A malicious user with upload permissions to the target host can cause a buffer overflow by uploading a \*.lnk file containing a certain value. When an LS command is issued on this directory, the buffer overflow allows the stack to be overwritten as well as the return address, causing code of the attacker's choosing to be executed on the local host with the same level of permissions as the EFTP process.
- Alternatively, the attacker could also use this exploit to cause a denial of service by having the exploit code continually execute a command such as querying the floppy drive of the target host.

### SAFER

- We are not aware of any solutions for this issue.

---

## Microsoft Windows NT RPC Endpoint Mapper Denial of Service Vulnerability

---

**Released** September 10, 2001

**Affects** Microsoft Windows NT 4.0 up to SP6 and NT Terminal Server

**Reference** <http://www.securityfocus.com/cgi-bin/vulns-item.pl?section=info&id=3313>

### Problem

- Remote Procedure Call (RPC) services are typically used by distributed applications such as SQL server and Exchange server. RPC services are assigned TCP and UDP ports dynamically. The RPC Endpoint Mapper service provides a mapping between RPC services and their currently assigned ports. Therefore, when a client requires access to a service using RPC, it must first request a port mapping from the RPC Endpoint Mapper, then it communicates directly with the service.
- When the RPC Endpoint Mapper, which typically resides on port 135, is sent a particular type of malformed data, it can cause the service to fail. This will cause all client attempts to communicate with RPC services on the target host to fail, resulting in a denial of services.
- The service can be restored to normal operation after a reboot of the server.

### SAFER

- Microsoft has released a hotfix which addresses this issue.

---

## DLink IP Fragment Denial Of Service Vulnerability

---

**Released** September 06, 2001

**Affects** D-Link DI-704 V2.56b5

**Reference** <http://www.securityfocus.com/cgi-bin/vulns-item.pl?section=info&id=3306>

### Problem

- A problem in the DI-704 may make it possible for a remote user to deny access to and from networks serviced by the router. The problem is due to the handling of fragmented IP packets.
- Upon receiving a high amount of fragmented IP packets over a period of two minutes, the router becomes unstable. Typically, this traffic will consume 100 percent of the CPU, starving the system of resources.
- However, after passing a period of time (reportedly two minutes), the router becomes unstable, and ceases function. The end result is the router ceasing operation, and requiring a reboot to resume normal function.

### SAFER

- Upgrade is available.

---

## NetBSD ioctl Denial of Service Vulnerability

---

**Released** September 06, 2001

**Affects** NetBSD 1.4 up to 1.5.1 and current pre20010805

**Reference** <http://www.securityfocus.com/cgi-bin/vulns-item.pl?section=info&id=3297>

### Problem

- The problem is the result of input validation errors in the ioctl(9) routines provided by several drivers included in the kernel. It is likely that the ioctl routine fails to properly check a user-supplied value used to allocate kernel memory or copy data from user memory. This might be accomplished by passing a large numeric value to the function and causing a signed integer overflow.
- If exploited, it may be possible for a local user to cause a kernel panic, requiring the machine to be reset. Additional technical details are forthcoming.

### SAFER

- Vendor-supplied updates that rectify this issue are available.

---

## Marconi ForeThought 7.1 Telnet Administration Denial of Service Vulnerability

---

**Released** September 04, 2001

**Affects** Marconi ForeThought 7.2

**Reference** <http://www.securityfocus.com/cgi-bin/vulns-item.pl?section=info&id=3286>

### Problem

- The telnet administration interface allows up to two concurrent sessions. When both sessions are locked, the only way to release the sessions is to reboot the device. Until the device is rebooted, access to the telnet interface is not possible.
- It has been reported that some port scans may unintentionally trigger this condition.

### SAFER

- We are not aware of any solutions for this issue.

# UNDERGROUND TOOLS

Here are the new tools that hackers/crackers will soon use against your systems. We do not recommend that you use such tools against any resources without prior authorization. We only list new tools published since the last issue of SAFER.

## SCANNERS

**NONE**

NONE

## EXPLOITS

**hp-swverify.c**

Exploit for HP-UX SWVerify Buffer Overflow Vulnerability

**msgchkx.c**

Exploit for Digital Unix MSGCHK Buffer Overflow Vulnerability

**msgchkx.sh**

Exploit for Digital Unix MSGCHK MH\_PROFILE Symbolic Link Vulnerability

**Eftpsizemap.pl**

Exploit for EFTP Server Directory and File Existence Vulnerability

**apachex.php**

Exploit for Red Hat Linux Apache Remote Username Enumeration Vulnerability

**homebetlog.pl**

Exploit for AmTote Homebet World Accessible Log Vulnerability

**ba.pl**

Exploit for Amtote Homebet Account Information Brute Force Vulnerability

**cso.c**

Exploit for cgicso included with cgiemail 1.6

## DENIAL-OF-SERVICE

**jolt2.c**

Exploit for DLink IP Fragment Denial Of Service Vulnerability

**ex\_eftpd.c**

Exploit for EFTP Buffer Overflow Code Execution and Denial of Service Vulnerability

**DoSadsl812.java**

Denial of service attack against a 3com ADSL 812 router

## PASSWORD CRACKERS

**iws\_pwc.c**

iPlanet/Netscape Enterprise Web server admin password cracker (for SHA1 hashes)

## OTHER

**ettercap-0.6.0.tar.gz**

Ettercap is a network sniffer/interceptor/logger for switched LANs