

**S·A·F·E·R**

**SECURITY ALERT FOR ENTERPRISE RESOURCES**

**Volume 2 Issue 4**

**April 1999**

*A monthly publication of Siam Relay Ltd. Copyright © 1999 All rights reserved.  
For further information or comments please contact [security@siamrelay.com](mailto:security@siamrelay.com)*

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

SAFER subscriptions can be made at <http://safer.siamrelay.com>

# CONTENTS

<b>CONTENTS</b> .....	<b>2</b>
<b>EXECUTIVE NEWS</b> .....	<b>3</b>
GENERAL NEWS .....	3
EUROPE – MIDDLE-EAST .....	3
UNITED STATES - CANADA .....	4
ASIA - PACIFIC .....	4
<b>LETTERS TO THE EDITOR</b> .....	<b>5</b>
<b>SECURITY ALERTS</b> .....	<b>6</b>
XYLAN OMNISWITCH SECURITY PROBLEMS.....	6
XFS (FONT SERVER) SECURITY BUG.....	6
XFREE86 X-WINDOWS SERVER VULNERABILITY.....	6
MICROSOFT SITE SERVER 3.0 WITH DIRECTMAIL.....	6
LOTUS NOTES CLIENT 4.5 ENCRYPTION FLAW .....	7
"\??" OBJECT SECURITY VULNERABILITY IN WINDOWS NT .....	7
WINDOWS NT SCREEN SAVER VULNERABILITY .....	7
ISAPI EXTENSION VULNERABILITY .....	7
BUFFER OVERFLOW IN /USR/BIN/CANCEL ON SOLARIS .....	8
IMAIL STORES PASSWORDS IN INSECURE WAY .....	8
<b>SECURITY ADVISORIES</b> .....	<b>9</b>
ISS SECURITY ADVISORY: WEBRAMP DENIAL OF SERVICE ATTACKS .....	9
HEWLETT-PACKARD SECURITY BULLETIN: #00096.....	9
HEWLETT-PACKARD SECURITY BULLETIN: #00095.....	9
REDHAT SECURITY: VARIOUS PACKAGES UPDATED (PINE, MUTT, SYSKLOGD, ZGV).....	9
SUSE SECURITY ANNOUNCEMENT: XFREE86 .....	10
CIAC BULLETIN J-037: W97M.MELISSA WORD MACRO VIRUS.....	10
MICROSOFT SECURITY BULLETIN (MS99-010).....	10
LOTUS NOTES SECURITY ADVISORY .....	10
HEWLETT-PACKARD SECURITY BULLETIN: #00094.....	11
ISS SECURITY ADVISORY: REMOTE DENIAL OF SERVICE IN CISCO CATALYST SERIES ETHERNET SWITCHES... ..	11
CISCO SECURITY NOTICE: CISCO CATALYST SUPERVISOR REMOTE RELOAD .....	11
OPENSSL/SSLEAY SECURITY ALERT .....	11
SUSE SECURITY ANNOUNCEMENT: THE DEFAULT PERMISSIONS ON /DEV/KMEM IS INSECURE .....	12
SUSE SECURITY ANNOUNCEMENT: A HOLE IN NETSCAPE COMMUNICATOR'S 4.5 "TALKBACK" FUNCTION .....	12
NETBSD SECURITY ADVISORY 1999-007 .....	12
NETBSD SECURITY ADVISORY 1999-006 .....	12
HEWLETT-PACKARD SECURITY BULLETIN: #00093.....	13
ISS SECURITY ADVISORY: SLACKWARE 3.6 NETWORK INSTALLATION PROBLEMS .....	13
MICROSOFT SECURITY BULLETIN (MS99-009).....	13
ISS SECURITY ADVISORY: LDAP BUFFER OVERFLOW AGAINST MICROSOFT DIRECTORY SERVICES.....	13
MICROSOFT SECURITY BULLETIN (MS99-008).....	14
ISS SECURITY ADVISORY: REMOTE RECONFIGURATION / DENIAL OF SERVICE IN CISCO 700 ROUTERS .....	14
CISCO 7XX TCP AND HTTP VULNERABILITIES .....	14
NAI SECURITY ADVISORY: LINUX BLIND TCP SPOOFING .....	14
SGI SECURITY ADVISORY 19990301-01-PX: X SERVER FONT PATH BUFFER OVERFLOW VULNERABILITY .....	15
HEWLETT-PACKARD SECURITY BULLETIN: #00092.....	15
<b>DENIAL-OF-SERVICE</b> .....	<b>16</b>
DoS FOR LINUX 2.1.89 - 2.2.3: 0 LENGTH FRAGMENT BUG.....	16
64 BIT SOLARIS 7 PROCFS BUG .....	16
MULTIPLE IMAIL VULNERABILITIES .....	16
<b>SECURITY BUGS</b> .....	<b>17</b>
<b>UNDERGROUND TOOLS</b> .....	<b>19</b>
<b>OVERGROUND TOOLS</b> .....	<b>21</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

---

- [www.nato.int](http://www.nato.int) and [www.whitehouse.gov](http://www.whitehouse.gov) **have been hacked by Russian hackers** as a sign of protest against NATO strikes on Yugoslavia. It seems that even the most protected sites are still very vulnerable to hackers with the appropriate motivation. NATO didn't say anything about the hack, and The White House claimed a hardware crash was the cause of the site being down for almost 2 days.
- **Kevin Mitnick ended his forty-nine month battle with the Government** by pleading guilty to some charges arising from his activities as a computer hacker. It is worth mentioning that Mitnick has been held in jail for 4 years, without having a trial.
- **A free e-mail program called ProMail is stealing users' names and passwords** and sending them to an unknown person. The recipient is presumably the creator of what is termed a "Trojan horse" virus. A teenager called "David" has claimed responsibility in an e-mail to Ken Williams, who runs Packet Storm Security, a Web security site.
- We have heard that **certain companies are organizing "hacking classes"**, where they guarantee to teach beginners how to hack, within a few days. It usually takes a few years to become a "hacker", but it seems that the human race is evolving very quickly. As long as you can pay, you will skip the years of learning and even get a diploma. Will we soon see "*Certified Hacker*" in signatures?

---

## Europe – Middle-East

---

- Much noise was created around the story alleging that **hackers seized control of one of Britain's military communication satellites** and issued blackmail threats. A newspaper, quoting security sources, said the intruders altered the course of one of Britain's four satellites which are used by defense planners and military forces around the world. It could have happened, it could be an inside job. Or it could be another journalistic sensationalism. It certainly raises the increasingly concerning issue of critical information resources, such as defense systems, exposed to electronic compromise.
- **The British government has asked businesses and civil servants to help protect the country from a cyberattack.** In a London conference, closed to the media, the leader of the House of Commons, Margaret Beckett, warned those responsible for running vital telecommunications, electricity, and health care networks for the country that they must make those systems more secure because of the increasing interconnectivity of networks and more cracker opportunities.

---

## United States - Canada

---

- **The military's key communications infrastructure linking combat, intelligence and command forces** is dangerously vulnerable to attacks from cyberspace and requires urgent changes in Defense Department policy. The Command, Control, Communications, Computers and Intelligence systems, known as C4I, are vulnerable because of security problems and also by a military culture prone to treating such problems as a lesser priority, the National Research Council reported.
- The Pentagon has **launched a probe on efforts by computer hackers based in Russia to access sensitive U.S. defense computers**. The report noted past attempts by outsiders to breach the computers but said "this time the Pentagon believes there is something unusually serious going on." We were always wondering how government officials know where attacks are really originating from.
- **The FBI released an annual survey** that it conducts with the San Francisco-based Computer Security Institute, reporting that criminal hacking caused \$123 million in losses last year, and now posed "a growing threat to the rule of law in cyberspace."
- **Microsoft Corporation moved to defuse a potentially explosive privacy issue**, saying it would modify a feature of its Windows 98 operating system that has been quietly used to create a vast database of personal information about computer users. Thank you Microsoft... now we feel much more secure...

---

## Asia - Pacific

---

- **Australia's domestic spy agency, ASIO, will be given sweeping powers to hack into computers and place tracking devices on people and cars**. In the most far-reaching upgrade in a decade to ASIO's powers, the agency will also be permitted to collect foreign intelligence in Australia and pass the information to the Australian Secret Intelligence Service (ASIS), the foreign spy agency.

# LETTERS TO THE EDITOR

***“ What are the security issues worth considering with the processing of credit card on the Internet? “***

Electronic commerce is experiencing a real boost. Analysts predict that 8 billion US\$ will be transferred in year 2001 through Electronic Commerce (Business-To-Business). However, responsibilities must be taken by those who provide on-line stores.

If you ask someone who never purchased an item over the Internet: “Why haven’t you?”, the most common answer would be, “I am afraid that someone will steal my credit card number”. For those who are aware as to how Electronic Commerce works, this sounds slightly absurd. How many times did that person give their credit card to a waiter in a restaurant? Or to a salesperson in a shop? The chances that someone will steal your credit card number are much higher in the “real world” than on the Internet. Furthermore, the customer is also protected by the credit card company.

But, danger still exists.

## ***Storage of credit card numbers***

Whether an on-line shop is processing credit cards in real time or in batches, it is possible that at some point during or after the authorization process, the credit card details are stored on a hard disk. There is a chance that a hacker can obtain access to the site, and just pick up the credit card numbers periodically. Until the administrator finds him (if ever). This is far more productive than trying to pick up numbers as they travel across the Internet.

Even some big-traffic online sites are keeping the numbers on the hard disk. This can make things easier for the customer, so that they don’t have to enter their credit card details each time an order is submitted. However, usually this information should be encrypted on the hard drive, and so if a hacker gets access to it, it is difficult to decrypt the data. Nevertheless the possibility is there.

## ***Unencrypted traffic***

There are still sites that do not use SSL when transferring sensitive information, such as credit card details. The traffic can be sniffed by a third party while in transit, and no cracking is needed at all. Often, sites claim that security is in place, but customers do not know how to check it.

## ***Careless employees***

When credit cards are authorized in batches, employees can be printing out details. Papers can be thrown in the garbage, and are then available for hackers to “trash” (going through garbage to find information). This also applies to password and other sensitive information.

## ***Merchants Liability***

Visa now claim the highest percentage of fraud is from Internet transactions, the amount being 2% of total turnover. This means that the merchant is at as much risk as the customer, if not more. There are methods to decrease the chance of fraud; Using address verification (only good for customers in the States), software is also available to screen information and search for common fraud signs. Merchants may also want to use only a courier to deliver goods so that the order can be traced to a recipient in the event of a fraud claim.

# 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.*

---

## Xylan OmniSwitch security problems

---

**Released** March 31, 1999

**Affects** Xylan OmniSwitch with software versions up to (and including) 3.1.8

**Reference** [http://geek-girl.com/bugtraq/1999\\_1/1191.html](http://geek-girl.com/bugtraq/1999_1/1191.html)

### Problem

- Anyone can telnet to the switch and login, without knowing either user or password strings. However, no permission will be given to perform any commands (it is possible that more security issues exist with this bug).
- Anyone can ftp to the switch, without knowing either user or password strings. Everyone is allowed to read all files in the flash, and even upload files.

### SAFER

- SNMP community string can also be easily obtained (if logged to ftp service).

---

## Xfs (font server) security bug

---

**Released** March 30, 1999

**Affects** XFree 3.3.3 on various platforms

**Reference** <http://www.xfree86.org>

### Problem

- Normal user can change permissions on system files by creating /tmp/.font-unix and waiting for root to start xfs.

### SAFER

- Only permission on the files can be changed (to world writable) – no files can be deleted.

---

## XFree86 X-Windows server vulnerability

---

**Released** March 26, 1999

**Affects** NetBSD/Linux (confirmed); possibly other platforms

**Reference** <http://www.xfree86.org>

### Problem

- User can modify permission on system files by creating /tmp/.X11-unix file and starting X server.

### SAFER

- If /tmp/.X11-unix already exists, the system can not be compromised.

---

## Microsoft SiteServer 3.0 with DirectMail

---

**Released** March 26, 1999

**Affects** Windows NT

**Reference** <http://ntbugtraq.ntadvice.com/default.asp?pid=36&sid=1&A2=ind9903&L=NTBUGTRAQ&P=R3469>

### Problem

- When DM (DirectMail) job is started, it creates a file that contains the username/password in clear text.

### SAFER

- Everyone has read access to that file, and can gain administrative privileges in an easy way.

---

## Lotus Notes Client 4.5 encryption flaw

---

**Released** March 23, 1999

**Affects** Lotus Notes client 4.5 (possibly others)

**Reference** [http://geek-girl.com/bugtraq/1999\\_1/1113.html](http://geek-girl.com/bugtraq/1999_1/1113.html)

### Problem

- Under certain circumstances, when user is sending an encrypted mail, the copy of the mail will be stored on the main server – unencrypted.

### SAFER

- Lotus has been notified of this issue, and is working on a fix.

---

## "\??" object security vulnerability in Windows NT

---

**Released** March 13, 1999

**Affects** Windows NT computers

**Reference** <http://www.cybermedia.co.in/>

### Problem

- Case Sensitivity vulnerability exists in Microsoft's Windows NT operating system.
- This security hole allows user to get "Administrator" access on a machine while logged in as "guest" or any ordinary user.

### SAFER

- The sample code to exploit this vulnerability has been made public.

---

## Windows NT Screen Saver Vulnerability

---

**Released** March 9, 1999

**Affects** Windows NT 4 (SP1), Windows 2000 Beta 1 and Beta 2

**Reference** <http://www.cybermedia.co.in/>

### Problem

- The screen saver is started by Winlogon.Exe, and once it gets the process handle to screen saver, it changes the primary security token of the screen saver to that of the logged in user and then resumes the screen saver process.
- The Winlogon.Exe does not check whether the changing of Primary token is successful. If setting of primary token fails due to some reason, the screen saver binary will run in system context.

### SAFER

- The sample code to exploit this vulnerability has been made public.

---

## ISAPI Extension vulnerability

---

**Released** March 8, 1999

**Affects** Web servers offering ISAPI support (running on Windows NT platform)

**Reference** [http://geek-girl.com/bugtraq/1999\\_1/0957.html](http://geek-girl.com/bugtraq/1999_1/0957.html)

### Problem

- A vulnerability exists in IIS (and other WEB servers executing as SYSTEM) that allows user to execute an ISAPI extension in the security context of the server itself.

### SAFER

- Many ISPs are being affected with this bug, since most ISPs that are providing services on NT are also providing ISAPI extension support.

---

## Buffer overflow in /usr/bin/cancel on Solaris

---

**Released** March 5, 1999

**Affects** Solaris 2.6

**Reference** <http://sunsolve.sun.com/sunsolve/secbulletins>

### Problem

- Buffer overflow exists in 'cancel' program that can potentially enable local user to obtain root privileges.
- No malicious code has been made public yet, and it is not yet known if this overflow can really be exploited in order to obtain root privileges.

### SAFER

- Sun is working on the patch.

---

## IMAIL stores passwords in insecure way

---

**Released** March 4, 1999

**Affects** IMAIL SMTP server

**Reference** [http://geek-girl.com/bugtraq/1999\\_1/0932.html](http://geek-girl.com/bugtraq/1999_1/0932.html)

### Problem

- IMAIL is storing the password in the registry, and those registry keys are world readable
- Encryption method used is very simple.

### SAFER

- No updates are available yet.

# SECURITY ADVISORIES

*This section contains official advisories as released by various vendors or security organizations. This list addresses the problems found during March 1999.*

---

## ISS Security Advisory: WebRamp Denial of Service Attacks

---

**Released** March 31, 1999

**Affects** WebRamp users

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

### Problem

- WebRamp is vulnerable to two denial of service attacks that allow an attacker to either crash the WebRamp device or change its IP address.
- Sending a specially formatted string of characters to the HTTP port of the WebRamp causes the device to hang, requiring a manual reset.
- Sending a specially-formatted UDP packet to port 5353 changes the WebRamp's local IP address

### SAFER

- We notice that Ramp Networks have already denied the existence of some serious bugs. We hope that now these bugs are clear enough.

---

## HEWLETT-PACKARD SECURITY BULLETIN: #00096

---

**Released** March 31, 1999

**Affects** MC/ServiceGuard & MC/LockManager

**Reference** <http://us-support.external.hp.com>

### Problem

- MC/ServiceGuard and MC/LockManager exhibit improper implementation of restricted SAM functionality.
- Users can increase their privileges.

### SAFER

- HP have issued patches for this problem.

---

## HEWLETT-PACKARD SECURITY BULLETIN: #00095

---

**Released** March 31, 1999

**Affects** HP-UX 10.20 and 11.00 with Domain Enterprise Server Management System running

**Reference** <http://us-support.external.hp.com>

### Problem

- Domain Enterprise Server Management System (DESMS) processes allow increased privileges.
- Users can gain increased privileges.

### SAFER

- HP have issued patches for this problem.

---

## RedHat Security: various packages updated (pine, mutt, syslogd, zgv)

---

**Released** March 30, 1999

**Affects** RedHat Linux distributions (possibly others platforms and distributions)

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

### Problem

- Problems have been found in a few programs that are delivered with RedHat Linux.
- Unauthorized root access and Denial-Of-Service problems have been fixed.

### SAFER

- As usual, problems have been fixed quickly.

---

**SuSE Security Announcement: XFree86**

---

**Released** March 28, 1999

**Affects** UNIX operating systems using XFree86

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

**Problem**

- A security hole was discovered in the Xfree86 package.
- A local attacker may create files with any contents in any directory.

**SAFER**

- SuSE reacted quickly, and updated the problematic package.

---

**CIAC Bulletin J-037: W97M.Melissa Word Macro Virus**

---

**Released** March 27, 1999

**Affects** Windows 95/NT running Microsoft Word 97 (version 8) or Word 2000 (version 9) and Microsoft Outlook.

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

**Problem**

- Overwrites the first macro in open documents and in the normal.dot template with the macro virus code.
- Turns off macro detection in Word.
- Sends copies of the infected document to up to 50 people from each of Outlook address books.

**SAFER**

- The mutations of this virus are already in "the wild". We've seen reports of an alleged variant of this virus which supposedly would download a minimal Slackware Linux distribution and install it (overwriting the existing Windows installation);

---

**Microsoft Security Bulletin (MS99-010)**

---

**Released** March 27, 1999

**Affects** Microsoft Personal Web Server (as shipped with Win98 and NT Option pack 4)

**Reference** <http://www.microsoft.com/security/services/bulletin.asp>

**Problem**

- A vulnerability exists that allows a file request that uses a non-standard URL to bypass the server's normal file access controls.
- The vulnerability would allow files on the server to be read, but not changed or deleted, and would not allow new files to be written to the server.

**SAFER**

- Microsoft has issued a patch.

---

**Lotus Notes security advisory**

---

**Released** March 26, 1999

**Affects** Lotus Notes Client (R4.5 and Later)

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

**Problem**

- There is a bug in the Lotus Notes Client which causes encrypted email messages to be saved in the sender's mailbox in unencrypted form.
- The bug only occurs when the Notes client is "misconfigured".

**SAFER**

- Another "it's not our mistake" vulnerability...

---

**HEWLETT-PACKARD SECURITY BULLETIN: #00094**

---

**Released** March 25, 1999

**Affects** HP-UX 11.00

**Reference** <http://us-support.external.hp.com>

**Problem**

- During normal operations, the ftp program might grant users increased privileges.

**SAFER**

- This bug affects only HP-UX 11.00. HP has issued a patch.

---

**ISS Security Advisory: Remote Denial of Service in Cisco Catalyst Series Ethernet Switches**

---

**Released** March 24, 1999

**Affects** Catalyst 1200, 2900, 5000, and 5500 series switches

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

**Problem**

- The Cisco switch software operates an undocumented TCP service.
- Sending a carriage return character to this port causes the switch to immediately reset. An attacker may repeat this action indefinitely, causing a denial of network services.

**SAFER**

- Customers should download the new version of the switch software.

---

**Cisco security notice: Cisco Catalyst Supervisor Remote Reload**

---

**Released** March 24, 1999

**Affects** Catalyst 1200, 2900, 5000, and 5500 series switches

**Reference** <http://www.cisco.com/warp/public/770/cat7161-pub.shtml>

**Problem**

- A software bug allows remote TCP/IP users to cause reloads of Cisco Catalyst LAN switches.

**SAFER**

- New version of software is available.

---

**OpenSSL/SSLeay Security Alert**

---

**Released** March 22, 1999

**Affects** All server software using SSLeay or versions of OpenSSL prior to version 0.9.2b

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

**Problem**

- SSL sessions include a session ID which allows the initial setup to be bypassed once a session has been established between a client and server. Server software using SSLeay or versions of OpenSSL prior to version 0.9.2b
- It is sometimes possible for a specially written SSL client to fraudulently obtain an SSL connection which requires access control by reusing a previous session which had different or no access control.

**SAFER**

- Fixed version is out. Recompile the software.

---

**SuSE Security Announcement: The default permissions on /dev/kmem is insecure**

---

**Released** March 18, 1999

**Affects** Linux 2.0.35 (kernel) and below

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

**Problem**

- The default permissions on /dev/kmem are insecure. LSOF overflow can be used in conjunction with this problem in order to gain higher privileges.
- A bug in all Linux 2.0.x kernels prior to 2.0.36 have a vulnerability which makes blind IP-spoofing possible.

**SAFER**

- Download new packages from SuSE.

---

**SuSE Security Announcement: A hole in Netscape Communicator's 4.5 "talkback" function**

---

**Released** March 18, 1999

**Affects** UNIX operating systems using Netscape Communicator 4.5

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

**Problem**

- If Communicator crashes for any reason, the file with the name /tmp/.\${UID}.talkback is read in, and the pid in this file is killed.
- After that, the file is truncated/created without checks for symlinks/hardlinks and the pid of the current talkback process is written into the file.

**SAFER**

- Upgrade to Communicator 4.51

---

**NetBSD Security Advisory 1999-007**

---

**Released** March 18, 1999

**Affects** NetBSD 1.3.3 and prior; NetBSD-current until 19990318

**Reference** <http://www.NetBSD.ORG/Security/>

**Problem**

- Insufficient checks in the mount system call may allow a regular user to mount a device, remote host or local directory without the `noexec' option, allowing them to execute arbitrary binaries.

**SAFER**

- A patch is available for the NetBSD 1.3.3 which makes the mount system call inherit the `noexec' flag from the mount point.

---

**NetBSD Security Advisory 1999-006**

---

**Released** March 17, 1999

**Affects** NetBSD 1.3.3 and prior; NetBSD-current until 19990312

**Reference** <http://www.NetBSD.ORG/Security/>

**Problem**

- Insufficient kernel checking in the umapfs virtual file system allows local users to remap their user id to any other user including the root user.

**SAFER**

- A malicious user can compile their own mount\_umap binary, and user can mount any directory on another directory they have write access to with their uid mapped to 0.

---

**HEWLETT-PACKARD SECURITY BULLETIN: #00093**

---

**Released** March 17, 1999

**Affects** HP-UX 10.20

**Reference** <http://us-support.external.hp.com>

**Problem**

- PHSS\_13560 patch introduced a library access problem into hpterm, the terminal emulator for the X Window system.
- Users can gain increased privileges.

**SAFER**

- Patch is available from HP.

---

**ISS Security Advisory: Slackware 3.6 Network Installation problems**

---

**Released** March 17, 1999

**Affects** Slackware 3.6 distributions

**Reference** <http://sunsolve.sun.com/sunsolve/secbulletins>

**Problem**

- During routine installation of Slackware Linux, there may be a period of time during which the system being installed is vulnerable to remote root login via telnet or other services.
- The vulnerability exists if Slackware is installed with the "net.i" boot image or if a network enabled kernel is installed during the initial installation.

**SAFER**

- Updated packages are available from Slackware site.

---

**Microsoft Security Bulletin (MS99-009)**

---

**Released** March 16, 1999

**Affects** Microsoft Exchange 5.5

**Reference** <http://www.microsoft.com/security/services/bulletin.asp>

**Problem**

- Microsoft has released a patch that eliminates a vulnerability in the LDAP Bind function for Microsoft Exchange 5.5.
- The vulnerability could allow denial of service attacks against an Exchange server or, under certain conditions, could allow arbitrary code to be run on the server.

**SAFER**

- Customers can also reduce their vulnerability to attacks from external sources by filtering incoming packets destined for TCP port 389, the LDAP service port.

---

**ISS Security Advisory: LDAP Buffer overflow against Microsoft Directory Services**

---

**Released** March 15, 1999

**Affects** Microsoft Exchange Server 5.5

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

**Problem**

- ISS X-Force has discovered a buffer overflow exploit against Microsoft Exchange's LDAP (Lightweight Directory Access Protocol) server which allows read access to the Exchange server directory by using an LDAP client.
- This buffer overflow consists of a malformed bind request that overflows the buffer and can execute arbitrary code.

**SAFER**

- This attack can also cause the Exchange LDAP service to crash.

---

**Microsoft Security Bulletin (MS99-008)**

---

**Released** March 12, 1999

**Affects** Microsoft Windows NT 4.0

**Reference** <http://www.microsoft.com/security/services/bulletin.asp>

**Problem**

- A vulnerability exists that is affecting all versions of Microsoft Windows NT operating system, which could allow a user to gain administrative privileges on a computer.
- Windows NT initially launches a screen saver in the local system context, then immediately changes its security context to match that of the user. However, Windows NT does not check whether this context change was successfully made.

**SAFER**

- A sample code for this exploit has been publicly available.

---

**ISS Security Advisory: Remote Reconfiguration / Denial of Service in Cisco 700 Routers**

---

**Released** March 11, 1999

**Affects** Cisco series 700 routers

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

**Problem**

- Remote attackers may issue commands to the router without authentication.
- Remote users may also deny network connectivity by forcing the router to reboot.

**SAFER**

- And so there are people who actually rely on security provided by routers...

---

**Cisco 7xx TCP and HTTP Vulnerabilities**

---

**Released** March 11, 1999

**Affects** Cisco series 700 routers

**Reference** <http://www.cisco.com/warp/public/770/7xxconn-pub.shtml>

**Problem**

- Two vulnerabilities exist in Cisco 700 series of routers
- The first vulnerability, can be used to cause system reloads, and therefore denial of service, using TCP connections to the routers' TELNET ports.
- Unless the HTTP server that comes with the router is explicitly disabled, it can be used to make changes to the router configuration, and/or to gain information about that configuration.

**SAFER**

- Updates are available at Cisco site.

---

**NAI Security Advisory: Linux Blind TCP Spoofing**

---

**Released** March 9, 1999

**Affects** Linux systems running kernels prior to 2.0.36

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

**Problem**

- An implementation flaw in the Linux TCP/IP stack allows remote attackers to forge TCP connections without predicting sequence numbers and pass data to the application layer before a connection is established.

**SAFER**

- Upgrade to 2.0.36 or newer (2.2.x)

---

**SGI Security Advisory 19990301-01-PX: X server font path buffer overflow vulnerability**

---

**Released** March 8, 1999

**Affects** All IRIX versions prior to 6.5.1

**Reference** <http://www.sgi.com/Support/security/security.html>

**Problem**

- A buffer overflow vulnerability has been discovered in the X server's font path which can lead to a root compromise.

**SAFER**

- X-Server is installed by default on all IRIX platforms, and this vulnerability should be considered as a 'high-risk', since details have been discussed publicly in various mailing lists and newsgroups.

---

**HEWLETT-PACKARD SECURITY BULLETIN: #00092**

---

**Released** March 4, 1999

**Affects** HP-UX 10.24 (VVOS) with VirtualVault A.03.50

**Reference** <http://us-support.external.hp.com>

**Problem**

- Under certain conditions, Netscape Enterprise Server (NES) version 3.6 exhibits excessive CPU resource utilization.

**SAFER**

- Patch is available.

# DENIAL-OF-SERVICE

*Denial-of-Service attacks are becoming an increasing concern. Below is a compilation of denial-of-service security problems found in March 1999.*

---

## DoS for Linux 2.1.89 - 2.2.3: 0 length fragment bug

---

**Released** March 24, 1999

**Affects** Linux kernel 2.1.89 – 2.2.3

**Reference** [http://geek-girl.com/bugtraq/1999\\_1/1079.html](http://geek-girl.com/bugtraq/1999_1/1079.html)

### Problem

- A remote attacker can effectively disable a target's IP connectivity.

### SAFER

- Exploit has been made publicly available.

---

## 64 bit Solaris 7 procfs bug

---

**Released** March 9, 1999

**Affects** Solaris 7 (64-bit)

**Reference** [http://geek-girl.com/bugtraq/1999\\_1/0987.html](http://geek-girl.com/bugtraq/1999_1/0987.html)

### Problem

- Every user (non-privileged or privileged) can crash the computer with command 'more /proc/self/psinfo'.

### SAFER

- No response from Sun.

---

## Multiple IMail Vulnerabilities

---

**Released** March 1, 1999

**Affects** IMail 5.0

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

### Problem

- The imapd login process does not do proper bounds checking on usernames and passwords, and therefore buffer overflow occurs when sending 1200 and 1300 characters with LOGIN command.
- Sending 2 strings of 2375 characters will make LDAP service go to 90 percent and take up most of the system resources.
- Sending 2045 to the IMonitor service (port 8181) crashes IMail server.
- 3000 characters to Web service (port 8383) will crash IMail server.
- Whois daemon (port 43) will crash after 1000 characters are sent.

### SAFER

- No comment.

# SECURITY BUGS

*Many security problems are too specific to become a full advisory. Below is a list of security problems discovered in various software during the month of March 1999, which we advise you to check against your IT environment.*

## **Windows NT BSOD**

A program has been made available (with source) that enables any user to crash Windows NT computer (locally). Nothing new...

## **Internet Explorer 5 allows reading and sending of local files**

There is a security bug in Internet Explorer 5.0, which allows reading and sending local files to a remote server. The problem is a bug in the DHTML edit control, which allows pasting a filename in a FILE object. When the form is submitted via JavaScript, the contents of the file are sent to a remote server.

## **Internet Explorer 5 security vulnerabilities**

An ActiveX control exists ("DHTML Edit control Safe for Scripting for IE 5") in IE5 that makes the clipboard public and allows cross-frame access.

## **....More Internet Explorer 5 problems**

IE 5, when installed, changes silently the setting for the cookies to "Accept always" no matter how it was in IE4 before. Also, IE 5 created a service called "COM+ Event System". So far, nobody knows what is this service intended for...

## **....Even more on Internet Explorer 5**

If user has an old cookie from some site on hard disk, and revisits that same site with the cookie setting adjusted to prompt for acceptance, no prompt is given, and the cookie is automatically written to disk anyway. Wow.

## **....And another Internet Explorer 5 problem...**

During the installation process of Internet Explorer 5, setup will disable screen saver and task scheduler. If (for any reason) installation fails, the screen saver and task scheduler will remain disabled (and really surprise the owner of the machine).

## **Windows NT date problems**

If administrator uses calendar function (from traybar) and advances the date by 1 month, for example, every event that occurs meanwhile (before hitting CANCEL) like login, printing and similar, will have the date advanced for 1 month. For example, if you do that on PDC and the accounts have expiration periods...

## **Windows NT daylight saving problem**

If an NT server is rebooted during the hour following the end of daylight savings period (time back 1 hour), it will lock up at either the logon screen or the blue kernel load screen. Cycling power will not fix this problem until 1 hour has passed since the transition period.

## **Oracle 8.0.3 Enterprise on NT**

During the creation of an Oracle database, the Database Assistant lets user create either a custom or typical (default) database. If "custom" database is selected, a brief look at the log file (lorant\database\spoolmain.log) will show that the master password is stored in clear text, and is readable by anyone.

## **Linux insmod bug/security vulnerability**

When insmod is called without a full path to the module to load, it checks a small path to find the module in question. By default, this path is the current directory followed by the /lib/modules/ hierarchy. In the widely distributed versions of the software ('insmod'), the module is not checked for root ownership.

## **Potential vulnerability in SCO TermVision Windows 95 client**

TermVision 2.1 package is used to integrate SCO into the Windows networking environment (appears as "UNIX Neighborhood" on the desktop). However, the encryption used for the communication between server (SCO) and the client (Win95/NT) is extremely simple, and user/pass combination can be retrieved easily.

## **Password and DOS Vulnerability with Testrack**

TestTrack, a bug tracking software has a number of security problems that allow an attacker to acquire userids and passwords in clear text. TestTrack also has an implementation flaw that allows anyone to peg the CPU of the machine running the TestTrack server to 100%.

### **Eudora Attachment Buffer Overflow**

If two messages are sent to an Eudora 4.1 user that have an attachment with a filename of around 231 characters or more, the next time the user checks mail, Eudora crashes.

### **Promail trojan**

ProMail v1.21, an advanced freeware mail program for Windows 95/98, is a trojan. It has been spread through several worldwide distribution networks (SimTel.net, Shareware.com and others) as proml121.zip. Prior to doing any other action, the program performs a check for a valid network connection which, if found, allows for the sending of all of the personal user data, including the user's password in encrypted format, to an account on NetAddress - a free email provider.

### **Lynx 2.8 overflow**

An IMG tag with a width of about 250 characters instantly crashes Lynx 2.8.1pre9 (and probably others).

### **Macromedia Shockwave 7 security hole**

A security loophole exists in Shockwave 7. Web plug-in was sending personal user information, including passwords, back to Macromedia.

### **Netscape Communicator 4.51 vulnerability**

There is a bug in Netscape Communicator 4.51, 4.5 and 4.08/WinNT (possibly others), which allows URLs to be sniffed from another window. The exploit uses the ability to execute JavaScript code from specially designed URLs in the javascript console window, when an error is deliberately invoked.

### **SMTP server account probing**

SMTP servers are probed for common names, presumably so that spam can then be targeted at them. The attacking machine connects and issues hundreds of RCPT TO: commands, searching a long list of common user names for ones that don't cause errors. It then compiles a list of target addresses to spam. Unfortunately, the attack, besides allowing the perpetrator to spam users, also brings SMTP servers to their knees.

### **Netscape find() problem**

There is a design flaw in Netscape Communicator 4.5/4.08 (probably in others too) which allows the following security exploits:

- Reading the parsed content of local HTML files (text the user sees on the screen)
- Reading user's cache
- Browsing directories

### **XCMail buffer overflow**

A simple buffer overflow exists in XCMail email client for UNIX. The bug appears when replying to a message with a long subject line, and only when autoquote is on

### **Bypassing Excel Macro Virus Protection**

A 'paper' has been made available with details on how to bypass Excel macro virus protection. For more information, visit: [http://geek-girl.com/bugtraq/1999\\_1/1147.html](http://geek-girl.com/bugtraq/1999_1/1147.html)

### **SCO UNIX PID prediction**

During the boot, files are created in the /tmp directory (/tmp/tps\$pid). However, the PID is same every time and user can create symlinks in order to remove system files (upon next reboot).

### **ICQ DoS**

New ICQ99a allows users to run an integrated web server. However, supplying any invalid command to the web server port will crash the ICQ.

# 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

### **nmap211.tgz**

More bugfixes and fingerprints in the new version of the ultimate network scanner. We simply have to say that Fyodor (the author of the scanner) did a wonderful job. nMap is a must for any system administrator.

### **ftpscan.c**

It will take a list of IP addresses from the file as an input and scan them searching for ftp server that accepts anonymous logins (and possibly have world writeable directories).

### **httpservertime-0.01.tar.gz**

Determines the name and version of remote HTTP server.

### **miffo-check.c.gz**

A utility to check a class B or Class C ip range for active computers, with an option to check for a special port, output of result to a file, etc. Only TCP port support right now.

### **httpdtype-0.05.tar.gz**

Determines the name and version of remote HTTP server.

### **wu-scan.c**

Modified imapd scanner that will now scan hosts for vulnerable wu-ftp ftp daemons.

### **wuscan.c**

New scanner that scans hosts for vulnerable wu-ftp ftp daemons.

### **cgichk-11b.c**

CGI vulnerability scanner.

### **soupscan.c**

Fast and simple class C domain scanner.

## EXPLOITS

### **BEADMIN.ZIP**

Exploit source code for Windows NT screen saver vulnerability.

### **BeSysAdm.zip**

Exploit source code for Windows NT Case Sensitivity vulnerability.

### **cancelex.c**

Exploits /usr/bin/cancel buffer overflow on Solaris.

### **count.cgi.l.c**

Linux x86 exploit for Count.cgi

### **dip2.c**

Exploit for dip3.3.7o

### **forthack.exe**

This program will bypass any security which is supposed to be gained using Fortress. The program will change the Fortress password.

### **fortrvlr.exe**

Another program to bypass Fortress security.

**isapi.sploit.cpp**

Sample exploit code for the ISAPI extension vulnerability in Microsoft IIS.

**lin35.c**

Exploits the vulnerabilities (blind spoofing) in Linux kernel prior to 2.0.36

**new\_login.c**

Patched login.c that will allow user to login with any username (and special password). Will also log other users' passwords.

**receive.c**

Sample code for the "blind spoofing" vulnerability for Linux kernels prior to 2.0.36

**sbouncer004b.c**

Uses WinGate or SOCKS server for bouncing

**sco-filewiper.sh**

Exploits the vulnerability in SCO UNIX, where filenames in the /tmp directory are predictable, and upon next reboot, the chosen files will be deleted.

**wh0a.c**

WU-FTPD remote buffer overflow exploit.

**wuftp-exp.c**

Another WU-FTPD remote buffer overflow exploit.

**DENIAL-OF-SERVICE****InetdDoS-spewfing.tgz**

Denial-Of-Service against InetD.

**winfreeze.c**

Exploit that uses 'ICMP/Redirect-host message' packets to freeze Win9x/NT.

**winfreeze-sparc.c**

Exploit that uses 'ICMP/Redirect-host message' packets to freeze Win9x/NT (compiles on Solaris).

**0len.c**

Exploit code for 'zero-length-fragment' vulnerability on Linux.

**PASSWORD CRACKERS****gammaprog152.tgz**

Bruteforce password cracker for web based e-mail addresses.

**hintcrack.zip**

HintCrack is a tool to crack hotmail 'hints' using a dictionary attack..

**altine-cracker-1.05.00.tar.gz**

Saltine Cracker v1.05 is a TCP/IP Distributed Network Password Auditing Tool.

**ntsweep.zip**

NT password cracker

**OTHER****gma-click.c**

Very configurable utility that will enable someone to use WinGate servers in order to generate "valid" banner clicks (mostly used for porn sites and similar).

**guideonv1.exe**

Removes the GUID (Global Unique Identifier) from documents created with Microsoft products.

# OVERGROUND TOOLS

Since we tell you what the hackers are using – we thought it might be interesting to let you know of new tools which can help protect your systems

## AUDIT /IDS (NT)

### **cybersensor.zip**

<http://www.cybermedia.co.in/>

CyberSensor enables spying on any WIN32 API call.

### **AFind.exe**

<http://www.ntobjectives.com/>

A tool that lists files by their last access time.

## AUDIT/IDS (UNIX)

### **hostsentry-0.02.tar.gz**

<http://www.psionic.com/abacus/hostsentry/>

HostSentry is a host based intrusion detection tool that performs Login Anomaly Detection (LAD). This tool allows administrators to spot strange login behavior and quickly respond to compromised accounts and unusual behavior. HostSentry incorporates a dynamic database and actually "learns" the user login behavior. This behavior is then utilized by modular signatures to detect unusual events.

### **vpnd-1.0.0.tar.gz**

<http://www2.crosswinds.net/nuremberg/~anstein/unix/vpnd.html>

vpnd is a daemon which connects two networks on network level either via TCP/IP or a (virtual) leased line attached to a serial interface. All data transferred between the two networks is encrypted using the non-patented free Blowfish encryption algorithm with a key length of up to 576 bits.

### **icmp-0.9.tar.gz**

<http://www.kalug.lug.net/stealth/>

Powerful tool to monitor/analyze ICMP traffic on the LAN.

### **bb109c.tar.gz**

<http://maclawran.ca/bb-dnld/>

Big Brother 1.09c is a combination of monitoring methods. Unlike SNMP where information is just collected and devices polled, Big Brother is designed in such a way that each local system broadcasts it's own information to a central location. Simultaneously, Big Brother also polls all networked systems from a central location. This creates a highly efficient and redundant method for proactive network monitoring.

### **netsaint-0.0.1.tar.gz**

<http://netsaint.linuxbox.com/>

NetSaint is a program that will monitor hosts and services on your network. It has the ability to email or page you when a problem arises and when a problem is resolved.

### **nettest-1.0.tar.gz**

<http://zorro.pangea.ca/~renec/nettest.php3>

Nettest is a Perl script which tests the integrity of a net connection. If the connection is down, it will either beep the speaker, send email, write in the system logs, or all of the above.

### **ntop-1.1cr6.tar.gz**

<http://www-serra.unipi.it/~ntop/>

Ntop is a Unix tool that shows the network usage

### **qps-1.6.3.tar.gz**

<http://www.nada.kth.se/~f91-men/qps/>

Visual Process Manager. X11 version of "top" or "ps" that displays processes in a window and lets you sort and manipulate them.

### **watchdog-4.4.tar.gz**

<http://sunsite.unc.edu/pub/Linux/system/daemons/watchdog/>

Watchdog is a daemon that monitors systems processes and loads, and will automatically reboot a server if the load rises above a defined level.

### **log-0.15.tar.gz**

<http://www.glue.umd.edu/~ajoshi/>

Ftpd log analyzer

### **iplog-1.7.tar.gz**

<http://sunsite.unc.edu/pub/Linux/system/daemons/watchdog/>

IPlog is a collection of daemons that log tcp, udp, and icmp traffic.

**ippl-1.4.0.tar.gz**<http://www.via.ecp.fr/~hugo/ippl/>

IPPL is a configurable IP protocols logger. It currently logs incoming ICMP messages, TCP connections and UDP datagrams. It is configured with Apache-like rules and has a built-in DNS cache.

**syslog-ng-1.0.4.tar.gz**<http://www.balabit.hu/products/syslog-ng.html>

Syslog-ng is a syslogd replacement that adds greater functionality to logging.

**scandetd.c**<http://wizard.ae.krakow.pl/~mike/>

Scandetd is a port scan detection daemon

## SECURITY SCANNERS (UNIX)

**Nessus**<http://www.nessus.org>

Nessus is a free, open-sourced and easy-to-use security auditing tool for Linux, BSD and some other systems. It is multithreaded and plugin based, and has a nice X11 interface.

**SAINT**<http://www.wwdsi.com/saint>

SAINT (Security Administrator's Integrated Network Tool) is a security assessment tool based on SATAN. Features include scanning through a firewall, updated security checks from CERT & CIAC bulletins and a feature rich HTML interface.