



Newsletter
Issue 118 - 08.07.2002
<http://net-security.org>

This is a newsletter delivered to you by Help Net Security. It covers weekly roundups of security events that were in the news the past week. Visit Help Net Security for the latest security news - <http://net-security.org>.

=====

SPI Dynamics ALERT:
Learn how to outsmart the Top 14 Web Application hacks!

=====

ALERT: Test and assess your Web Applications TODAY! Hackers exploiting Web applications gain entry to backend data via Port 80 and 443! Firewalls and IDS don't stop these attacks because hackers using the Web App Layer are NOT seen as intruders.

Are you vulnerable? 15-Day *Free* Trial! Download now!
<http://www.spidynamics.com/mktg/freewebinspect5>

=====

Table of contents:

- 1) Security news
- 2) Vulnerabilities
- 3) Advisories
- 4) Virus news
- 5) Security world
- 6) Featured articles
- 7) Security software

[General security news]

KEVIN MITNICK WROTE A BOOK
"The Art of Deception" describes more than a dozen scenarios where tricksters dupe computer network administrators into divulging passwords, encryption keys and other coveted security details.

>> <http://www.net-security.org/news.php?id=494>

RELIGIOUS SECT HACKS CHINESE TV
Chinese religious sect Falun Gong successfully hijacked satellite TV broadcasts to homes in the Shandong province last week.

>> <http://www.net-security.org/news.php?id=495>

SEVEN COMMON SSL PITFALLS
This article discusses the seven most common pitfalls when

deploying SSL-enabled applications with OpenSSL.
>> <http://www.net-security.org/news.php?id=496>

BANK ACCOUNTS RAIDED IN SINGAPORE

Singapore's DBS Bank, the banking unit of DBS Group Holdings, says a computer hacker has siphoned money from 21 online bank accounts in amounts ranging from 73 to 1,800 pounds.
>> <http://www.net-security.org/news.php?id=497>

A PAPER ON VARIOUS ASPECTS OF SELINUX

This paper describes the security architecture, security mechanisms, application programming interface, security policy configuration, and performance of SELinux.
>> <http://www.net-security.org/news.php?id=498>

CANADA'S HERO HACKER UNMASKED

The mystery hacker whose online infiltration has led to several arrests of suspected child predators was a 19-year-old who penetrated 3,000 computers around the world from a basement in Langley, B.C.
>> <http://www.net-security.org/news.php?id=500>

INDIAN HACKERS CRACK PAKISTANI SITES

The Pakistan government's official website has been hit by Indian hackers, seemingly as part of a cyber turf war between rival groups.
>> <http://www.net-security.org/news.php?id=501>

WEB RIPE FOR MASSIVE WORM ATTACK

A new survey finds that the Web is more vulnerable to attack than ever before, due to the chance discovery of several vulnerabilities within days of one another.
>> <http://www.net-security.org/news.php?id=502>

DNS RESOLVER BUFFER OVERFLOW VULNERABILITY

A vulnerability exists in the DNS resolver library used by BSD and ISC BIND. An attacker who is able to control DNS responses could exploit arbitrary code or cause a DoS attack on vulnerable systems.
>> <http://www.net-security.org/news.php?id=504>

WHERE WIRELESS IS MOST VULNERABLE

This article shows four ways an attacker can hack the airwaves and get access to your network and beyond.
>> <http://www.net-security.org/news.php?id=505>

THE STATE OF ANOMALY DETECTION

This article offers a brief overview of anomaly detection, including what it is, how it works, different ADS techniques, and the current state of anomaly detection.
>> <http://www.net-security.org/news.php?id=506>

CYBERWAR IS HELL

The campaign against cyber terrorism has at least one thing in common with genuine conflicts: wartime profiteers.

>> <http://www.net-security.org/news.php?id=507>

REMOTE ACCESS DOESN'T HAVE TO BE A SECURITY RISK

Citrix iForum 2002 Africa, to be held on 23 July, will address how companies can go about securing the virtual workplace.

>> <http://www.net-security.org/news.php?id=508>

THE KEYS TO A MORE SECURE FUTURE

What are the factors that will determine how safe our world can be made? Here's a look at several, including some basic human qualities.

>> <http://www.net-security.org/news.php?id=509>

ZIMMERMANN WANTS PGP OPEN-SOURCED

"I would strongly prefer PGP be Open Source compared with the current scenario, because right now it's locked in intellectual property prison and no one can get it," he says. "Open Source would be much better."

>> <http://www.net-security.org/news.php?id=510>

COMPUTER VIRUSES MIMIC REAL THING

Computer and human viruses behave in similar ways, and the IT industry could ward off infections by adopting methods used by the medical profession, according to researchers.

>> <http://www.net-security.org/news.php?id=511>

WINDOWS 32 VIRUSES RULE THE WAVES

Sophos published an overview of the most common viruses reported in the first six months of 2002. During this period, the single most prevalent virus was Klez-H.

>> http://www.net-security.org/virus_news.php?id=41

CYBERSECURITY'S LEAKY DIKES

While interest is rising in protecting computer networks, too often the tools aren't powerful enough to keep hackers out.

>> <http://www.net-security.org/news.php?id=515>

ZONELABS: THE HOT STUFF IN FIREWALLS

Despite the tech doldrums, this computer-security outfit has just secured \$24.3 million in new VC funding, and sales are exploding.

>> <http://www.net-security.org/news.php?id=516>

SECURITY STEPS UP A NOTCH

An emerging subscription model for vulnerability scanning is breathing new life into security solution providers.

>> <http://www.net-security.org/news.php?id=517>

FBI TO VALLEY: TELL US ABOUT ATTACKS

Businesses don't report cyberattacks for fear that the bad publicity

would also bombard their bottom lines. The FBI now offers them anonymity and critical information in exchange for their cooperation.
>> <http://www.net-security.org/news.php?id=518>

SECURITY COMES FIRST FOR REMOTE WORKERS

Lots of users do significant amounts of work away from the office, either from their homes or on the road. Getting these users set up, supported and secured is a major challenge for IT.
>> <http://www.net-security.org/news.php?id=519>

MICROSOFT SECURITY PLAN SHOULDN'T SHUT OUT COMPETITORS

Microsoft should take care that its recently announced software security plan doesn't shut out competitors, the European Union's new antitrust enforcer said.
>> <http://www.net-security.org/news.php?id=520>

IDAR PROJECT PROTOTYPE

The Incident Detection, Analysis, and Response project has developed a prototype that demonstrates the feasibility of using a computer-based system to assist inexperienced system and network administrators during a network attack.
>> <http://www.net-security.org/news.php?id=522>

EUROPEANS BUST NET CHILD PORN RING

Police in seven European countries struck at a sophisticated child abuse and pornography ring dubbed "Shadowz Brotherhood," arresting 50 people and seizing computer equipment, CD-ROMs and videos.
>> <http://www.net-security.org/news.php?id=525>

HOW ONE SPAM LEADS TO ANOTHER

Once your e-mail gets on a spam list, you're basically doomed. Now there's a "map" that illustrates that doomsday path.
>> <http://www.net-security.org/news.php?id=526>

TWENTY DON'TS FOR ASP DEVELOPERS

Thinking securely is often an unnatural transition for programmers. While there is much to do when building a secure Web application, you can at least start with these twenty things you shouldn't do.
>> <http://www.net-security.org/news.php?id=527>

WHY E-COMMERCE LAW ENFORCEMENT IS AN OXYMORON

The Internet is simply too vast, stretching across too many borders and encompassing too many cultures, for the current scattershot approach to be effective.
>> <http://www.net-security.org/news.php?id=528>

KLEZ: THE VIRUS THAT WON'T DIE?

Brace yourself for another round: A variant of the resilient worm is wriggling alive this week.
>> <http://www.net-security.org/news.php?id=529>

HOW THE APACHE WORM COULD HAVE BEEN PREVENTED

Internet Security Services jumped the gun when it put out an all-points bulletin over a security hole in Apache servers. The resulting worm raises the question: When should we ring the alarms?
>> <http://www.net-security.org/news.php?id=530>

CYBERWAR

In global trouble spots, cells of "hacktivists" are waging e-war on rival states.
>> <http://www.net-security.org/news.php?id=532>

CORPORATE LAYOFFS CREATE SECURITY HAVOC FOR IT PROS

Big corporate layoffs are creating a nightmare of security risks as IT workers scramble to close down network connections and plug up dangerous holes as employees are walked out the door.
>> <http://www.net-security.org/news.php?id=533>

NEW APPROACH FOR ENCRYPTION

An unlikely combination of interests - cartoons and math - has inspired a sophomore at the University of Dayton to develop a new encryption technology.
>> <http://www.net-security.org/news.php?id=535>

HIDE MESSAGES IN IMAGES

Hacktivismo is developing a product called Camera/Shy capable of creating and displaying images with messages which would likely get a Web site shut down or filtered in some places.
>> <http://www.net-security.org/news.php?id=536>

SPAM-CRAMMING FOILS VACATIONERS

The spam epidemic is frustrating holiday-goers who vow not to read e-mail on the road. If they don't clear their inboxes, their ISPs may start rejecting the messages they want.
>> <http://www.net-security.org/news.php?id=537>

VIRGINIA BEACH TESTS FACIAL-RECOGNITION SOFTWARE

If you're a criminal, a runaway or a terrorist, a day at the beach here may soon be anything but that.
>> <http://www.net-security.org/news.php?id=538>

PERL ADVISOR: PARSING AND SUMMARIZING A LOGFILE

Randal L. Schwartz shows us how to create customized data reduction tools for log analysis.
>> <http://www.net-security.org/news.php?id=539>

MANAGED SECURITY TIPPED AS NEXT SUCCESS STORY

Although the local managed security services industry is still in its infancy, because of a shortage of IT security skills and budgetary pressures, managed services will become a growth area.
>> <http://www.net-security.org/news.php?id=540>

HACKER SWIPES \$35,000 FROM SING BANK

A Chinese national hacked into 21 online accounts at Singapore bank DBS, transferred \$35,000 into his own account, withdrew the money at a bank branch and then fled the country.

>> <http://www.net-security.org/news.php?id=541>

THE SECURITY CONCERNS OF LICENSING AGREEMENTS

This article discusses why security professionals need to be particularly aware of some issues that these licensing agreements present.

>> <http://www.net-security.org/news.php?id=542>

HOLDER WANTS TO STOP THE MCAFEE DEAL

A shareholder of McAfee.com Corp. filed a purported class-action lawsuit seeking an injunction to stop the company from being bought by its majority shareholder, Network Associates.

>> <http://www.net-security.org/news.php?id=543>

=====

Computer Security Institute Survey: 90% Say Systems Hacked.

How Secure Is Your Network? Get a FREE Assessment!

<http://www.net-security.org/lm/ads/ads.pl?banner=scannerx1>

=====

[Vulnerabilities]

All vulnerabilities are located here:

http://www.net-security.org/archive_vuln.php

Worldspan Denial of Service Vulnerability

>> <http://www.net-security.org/vuln.php?id=1843>

Remote Format String Vulnerability in nn

>> <http://www.net-security.org/vuln.php?id=1842>

Weak Cisco PIX Enable Password Encryption Algorithm

>> <http://www.net-security.org/vuln.php?id=1841>

Unreal Tournament Distibuted Denial of Service Risk

>> <http://www.net-security.org/vuln.php?id=1840>

OpenSSH kbd-interactive Buffer Overflow

>> <http://www.net-security.org/vuln.php?id=1839>

Argosoft Mail Server Plus/Pro Webmail Reverse Directory Traversal Vulnerability
>> <http://www.net-security.org/vuln.php?id=1838>

SunPCi II VNC Weak Authentication Scheme Vulnerability
>> <http://www.net-security.org/vuln.php?id=1837>

Remotely Exploitable Buffer Overruns in Microsoft's Commerce Server 2000/2
>> <http://www.net-security.org/vuln.php?id=1836>

PHPAuction Malicious Admin User Creation Vulnerability
>> <http://www.net-security.org/vuln.php?id=1835>

Commentary: Slashcode XSS Vulnerability
>> <http://www.net-security.org/vuln.php?id=1834>

CommuniGate Pro Directory Listings Vulnerability
>> <http://www.net-security.org/vuln.php?id=1833>

Noguska Nola 1.1.1 Malicious PHP Code Upload Vulnerability
>> <http://www.net-security.org/vuln.php?id=1832>

Slashcode Cross Site Scripting Vulnerability
>> <http://www.net-security.org/vuln.php?id=1831>

Jrun Sourcecode Disclosure Vulnerability
>> <http://www.net-security.org/vuln.php?id=1830>

Betsie Cross Site Scripting Vulnerability
>> <http://www.net-security.org/vuln.php?id=1829>

Sitespring Server Denial of Service Vulnerability
>> <http://www.net-security.org/vuln.php?id=1828>

OmniHTTPd 2.09 Buffer Overflow Vulnerability
>> <http://www.net-security.org/vuln.php?id=1827>

Blackboard 5 Cross Site Scripting Vulnerability
>> <http://www.net-security.org/vuln.php?id=1826>

Simple Wais 1.11 Allows Users to Execute Commands as SWAIS Daemon
>> <http://www.net-security.org/vuln.php?id=1825>

Macromedia JRun Admin Server Authentication Bypass Vulnerability
>> <http://www.net-security.org/vuln.php?id=1824>

WEB-INF Folder Accessible in Multiple Web Application Servers
>> <http://www.net-security.org/vuln.php?id=1823>

On-Line Whois Service Command Execution Vulnerability
>> <http://www.net-security.org/vuln.php?id=1822>

Xitami 2.5 Beta Errors.gsl Script Injection Vulnerabilities
>> <http://www.net-security.org/vuln.php?id=1821>

AnalogX SimpleServer:Shout Buffer Overflow Vulnerability
>> <http://www.net-security.org/vuln.php?id=1820>

[Advisories]

All advisories are located at:
http://www.net-security.org/archive_advi.php

Conectiva Linux Security Advisory - squid
>> <http://www.net-security.org/advisory.php?id=843>

Mandrake Linux Security Advisory - LPRng
>> <http://www.net-security.org/advisory.php?id=842>

Mandrake Linux Security Advisory - kernel 2.2 and 2.4
>> <http://www.net-security.org/advisory.php?id=841>

Red Hat Security Advisory - New Squid packages available
>> <http://www.net-security.org/advisory.php?id=840>

Conectiva Linux Security Advisory - ethereal
>> <http://www.net-security.org/advisory.php?id=839>

Cisco Security Advisory - Cisco Secure ACS Unix Acme.server
Information Disclosure
>> <http://www.net-security.org/advisory.php?id=838>

Compaq Security Bulletin - HP Tru64 UNIX V5.1a - SSH V1.1 &
OpenSSH Challenge Response Handling, Potential Security Vulnerability
>> <http://www.net-security.org/advisory.php?id=837>

Mandrake Linux Security Advisory - openssh (update)
>> <http://www.net-security.org/advisory.php?id=836>

Microsoft Security Bulletin MS02-029 - Unchecked Buffer in Remote Access Service Phonebook Could Lead to Code Execution (version 2.0)
>> <http://www.net-security.org/advisory.php?id=835>

Cisco Security Advisory - Cisco Secure ACS Unix Acme.server Information Disclosure
>> <http://www.net-security.org/advisory.php?id=834>

SuSE Security Announcement - openssh
>> <http://www.net-security.org/advisory.php?id=833>

Conectiva Linux Security Advisory - apache (mod_ssl)
>> <http://www.net-security.org/advisory.php?id=832>

EnGarde Secure Linux Advisory - off-by-one in mod_ssl's configuration directive handling
>> <http://www.net-security.org/advisory.php?id=831>

Microsoft Security Bulletin MS02-028 - Heap Overrun in HTR Chunked Encoding Could Enable Web Server Compromise (version 2.0)
>> <http://www.net-security.org/advisory.php?id=830>

Caldera Security Advisory - OpenServer 5.0.5 OpenServer 5.0.6: Apache Web Server Chunk Handling Vulnerability / mod_ssl off-by-one error
>> <http://www.net-security.org/advisory.php?id=829>

Caldera Security Advisory - UnixWare 7.1.1 Open UNIX 8.0.0: Apache Web Server Chunk Handling Vulnerability / mod_ssl off-by-one error
>> <http://www.net-security.org/advisory.php?id=828>

EnGarde Secure Linux Advisory - several vulnerabilities in the OpenSSH daemon
>> <http://www.net-security.org/advisory.php?id=827>

Compaq Security Bulletin - Secure Web Server for HP Tru64 UNIX & HP OpenVMS Potential Apache Web Server Chunk Handling Vulnerability
>> <http://www.net-security.org/advisory.php?id=826>

Debian Security Advisory - libapache-mod-ssl
>> <http://www.net-security.org/advisory.php?id=825>

NetBSD Security Advisory - buffer overrun in libc DNS resolver
>> <http://www.net-security.org/advisory.php?id=824>

NetBSD Security Advisory - OpenSSH protocol version 2
challenge-response authentication vulnerability
>> <http://www.net-security.org/advisory.php?id=823>

FreeBSD Security Advisory - Buffer overflow in resolver
>> <http://www.net-security.org/advisory.php?id=822>

Red Hat Security Advisory - Updated OpenSSH packages
fix various security issues
>> <http://www.net-security.org/advisory.php?id=821>

CERT Advisory CA-2002-19 - Buffer Overflow in Multiple
DNS Resolver Libraries
>> <http://www.net-security.org/advisory.php?id=820>

CERT Advisory CA-2002-18 - OpenSSH Vulnerabilities in
Challenge Response
>> <http://www.net-security.org/advisory.php?id=819>

Cisco Security Advisory - Scanning for SSH Can Cause a Crash
>> <http://www.net-security.org/advisory.php?id=818>

Caldera Security Advisory - Linux: OpenSSH Vulnerabilities in
Challenge Response Handling
>> <http://www.net-security.org/advisory.php?id=817>

Conectiva Linux Security Advisory - netsaint
>> <http://www.net-security.org/advisory.php?id=816>

Trustix Security Advisory - apache security fix
>> <http://www.net-security.org/advisory.php?id=815>

Trustix Security Advisory - openssh
>> <http://www.net-security.org/advisory.php?id=814>

Conectiva Linux Security Advisory - openssh
>> <http://www.net-security.org/advisory.php?id=813>

Conectiva Linux Security Advisory - nss_ldap
>> <http://www.net-security.org/advisory.php?id=812>

Debian Security Advisory - ssh (update 3)
>> <http://www.net-security.org/advisory.php?id=811>

[Virus News]

All virus news are located at:
<http://www.net-security.org/viruses.php>

Etap Author Tells Us The Score
>> http://www.net-security.org/virus_news.php?id=46

Sophos distributing W32/Yaha-E? Not guilty!
>> http://www.net-security.org/virus_news.php?id=45

Backdoor.K0wbot Analysis
>> http://www.net-security.org/virus_news.php?id=44

What's Coming?
>> http://www.net-security.org/virus_news.php?id=43

BSD.Worm.Scalper Analysis
>> http://www.net-security.org/virus_news.php?id=42

[Security world]

All press releases are located at:
http://www.net-security.org/press_main.php

Check Point Software's SmartDefense Named 'Hot Pick' by Information Security Magazine
>> <http://www.net-security.org/press.php?id=883>

New Certifications Reinforce Check Point Security Leadership
>> <http://www.net-security.org/press.php?id=882>

Symantec Acquires Mountain Wave, Inc.
>> <http://www.net-security.org/press.php?id=881>

Sophos And Talk-101 Converse To Combat Virus Threat
>> <http://www.net-security.org/press.php?id=880>

Intrusion Inc. Announces Second Quarter 2002 Results on
Thursday, July 18 2002

>> <http://www.net-security.org/press.php?id=879>

Content Security Company Cobion AG introduces OrangeBox Web V1.2

>> <http://www.net-security.org/press.php?id=878>

McAfee.com Advises Stockholders to Take No Action at This Time in
Response To Network Associates' Proposed Exchange Offer

>> <http://www.net-security.org/press.php?id=877>

Protegrity Secure.Data, Working With Microsoft Commerce Server And
Microsoft Sql Server 2000, Creates Enhanced Security And Privacy For
Internet Business

>> <http://www.net-security.org/press.php?id=876>

RSA Security Notice of Q2 2002 Earnings Release, Conference Call
and Webcast

>> <http://www.net-security.org/press.php?id=875>

Top South African Retail Center Uses CA Solutions To Develop
Innovative Customer Incentive Program

>> <http://www.net-security.org/press.php?id=874>

Abtrusion Security Announced Abtrusion Protector

>> <http://www.net-security.org/press.php?id=873>

Trusecure Named In The Top Ten Of The Fifty Fastest Growing
Companies In The Washington D.C. Region

>> <http://www.net-security.org/press.php?id=872>

nCipher's Hardware Security Module Designated with Entrust
Ready Status

>> <http://www.net-security.org/press.php?id=871>

[Featured articles]

All articles are located at:

http://www.net-security.org/articles_main.php

Articles can be contributed to staff@net-security.org

NETWORK INSECURITY

This technical brief will overview the inherent flaws that plague the internet today, making it vulnerable to corporate espionage, money laundering, grand larceny, trading frauds, and worst of all, cyber terrorism.

>> <http://www.net-security.org/article.php?id=141>

(MORE) ADVANCED SQL INJECTION

This paper addresses the subject of SQL Injection in a Microsoft SQL Server/IIS/Active Server Pages environment, but most of the techniques discussed have equivalents in other database environments.

>> <http://www.net-security.org/article.php?id=142>

INFORMATION SURVIVABILITY: REQUIRED SHIFTS IN PERSPECTIVE

Survivability, an emerging discipline, incorporates a new technical and business perspective on security, creating solutions that focus on elements such as the continuity of critical services. In terms of solution space, security takes a technology centric point of view, with each technology solving a specific set of issues and concerns that are generally separate and distinct from one another.

>> <http://www.net-security.org/article.php?id=143>

CREATING ARBITRARY SHELLCODE IN UNICODE EXPANDED STRINGS

This paper introduces a technique that can be used to permit the execution of a small amount of arbitrary code in a situation where a buffer overflow occurs in a "Unicode" string on the Intel x86 processors.

>> <http://www.net-security.org/article.php?id=144>

[Security Software]

Windows software is located at:
http://net-security.org/software_main.php?cat=1

Linux software is located at:
http://net-security.org/software_main.php?cat=2

LINUX TRUSTEES 2.9

The main goal of the Linux Trustees project is to create an advanced permission management system for Linux.

>> <http://www.net-security.org/software.php?id=179>

WINSSHD 3.05

WinSSHD is an SSH Secure Shell 2 server for Windows NT4, Windows 2000 and Windows XP.

>> <http://www.net-security.org/software.php?id=180>

TUNNELIER 3.03

Tunnelier is a powerful SSH2 port forwarding client with many features.

>> <http://www.net-security.org/software.php?id=181>

SSH-MULTIADD 1.3.2

ssh-multiadd adds multiple ssh keys to the ssh authentication agent.

>> <http://www.net-security.org/software.php?id=182>

FLAWFINDER 1.01

Flawfinder searches through source code looking for potential security flaws.

>> <http://www.net-security.org/software.php?id=183>

IDSA 0.93.1

IDSA is a combined system logger, reference monitor, and intrusion detection system for applications. An IDSA enabled application can not only be monitored, but also instructed to restrict functionality.

>> <http://www.net-security.org/software.php?id=184>

ANTI K0WBOT

This is a removal tool for another Internet worm that uses the file sharing KaZaA network to spread; besides this, it includes an IRC remote control backdoor component.

>> <http://www.net-security.org/software.php?id=185>

SYMBION SSL PROXY 1.0.0

The Symbion SSL Proxy listens on a TCP port, accepts SSL connections, and forwards them to another (local or remote) TCP port, or UNIX domain socket.

>> <http://www.net-security.org/software.php?id=186>

APASSWORD 1.0

APassword allows you to generate either single or batches of random passwords.

>> <http://www.net-security.org/software.php?id=187>

TIGHTVNC 1.2.4

TightVNC is a VNC distribution with many new features, improvements, and bugfixes over VNC.

>> <http://www.net-security.org/software.php?id=188>

SILC 0.94

SILC (Secure Internet Live Conferencing) is a protocol which provides secure conferencing services on the Internet over insecure channel.

>> <http://www.net-security.org/software.php?id=189>

Questions, contributions, comments or ideas go to:

Help Net Security staff
staff@net-security.org
<http://net-security.org>

Subscribe to this weekly digest on:

<http://www.net-security.org/subscribe.php>

Unsubscribe by sending your e-mail address to:

info@net-security.org with UNSUBSCRIBE in the message body.

The archive of the newsletter in TXT and PDF format is available

http://www.net-security.org/newsletter_archive.php