



Newsletter
Issue 120 - 22.07.2002
<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>.

SECURITY INCIDENT ALERT

43,136 security incidents have been reported through June, 2002. Last year 52,658 were reported for the entire year. The most common point of entry is exploitation of known operating system vulnerabilities.

Check your Web servers, FTP servers, Mail servers , DNS servers, firewalls, IDS systems, switchers and routers for over 900 up to date vulnerabilities. Secure your critical assets today!

FREE System Security Test and Detailed Report
<http://www.net-security.org/lm/ads/ads.pl?banner=scannerx1>

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]

LIBERTY ALLIANCE PROPOSES WEB SECURITY STANDARDS

A set of Sun Microsystems Inc-backed web services security specifications could soon pass to a standards-body backed by IBM and Microsoft, Gavin Clarke writes.

>> <http://www.net-security.org/news.php?id=596>

INTRUSION DETECTION: IMPLEMENTATION AND OPERATIONAL ISSUES

This article gives an overview of the most commonly used intrusion detection techniques.

>> <http://www.net-security.org/news.php?id=597>

CHEMICAL INDUSTRY DRAFTS CYBERSECURITY PLAN

The U.S. chemical industry has drafted a strategic plan for beefing up cybersecurity that also focuses on industrial control systems.

>> <http://www.net-security.org/news.php?id=598>

AT&T WARNS STAFF TO BE WARY OF HACKERS

AT&T has warned employees not to be tricked into surrendering sensitive information about its network to hackers posing as colleagues or customers.

>> <http://www.net-security.org/news.php?id=599>

HOMER SAYS HACK YOUR DVD PLAYER

Homer Simpson, cartoon character and a role model for millions, has been caught telling consumers to hack their DVD players.

>> <http://www.net-security.org/news.php?id=600>

CRYPTO CONTROLS ARE SPREADING INTERNATIONALLY

Hand over that encryption key, mate, monsieur, sir, bloke...

>> <http://www.net-security.org/news.php?id=602>

SECURELY INSTALLING LINUX

The best place to start cutting packages is in the communications area. You probably don't need an anonymous FTP server, or a telnet server, but they'll be installed if you're not careful...

>> <http://www.net-security.org/news.php?id=603>

CAN DATA SECURITY BE OUTSOURCED?

By understanding how ASPs (application service providers) protect your data, you may find it both more economical and safer to outsource your application and data management.

>> <http://www.net-security.org/news.php?id=605>

FDIC FAULTED FOR WEAK IT SECURITY

A federal agency created to help restore economic confidence during the Great Depression isn't winning the confidence of a congressional watchdog agency for its information security practices.

>> <http://www.net-security.org/news.php?id=606>

SECURITY WARS: CAN INTRUSION DETECTION EVEN THE SCORE?

Experts point to lingering gaps in areas that include accuracy, data interoperability, and analysis tools.

>> <http://www.net-security.org/news.php?id=607>

CABLE MODEMS - NOT JUST A SECURITY PROBLEM

As well as securing home-office cable connections, IT managers will have to deal with increased loads on corporate networks, and demands to support users at home.

>> <http://www.net-security.org/news.php?id=608>

H2K2 HACKERS SAY THEY WANT A REVOLUTION
But some charge that dot-com greed robbed the computer underground of its soul.
>> <http://www.net-security.org/news.php?id=609>

SECURITY SCANNING IS NOT RISK ANALYSIS
Many IT decision makers assume that performing a security vulnerability assessment is the same thing as risk analysis. However, these two processes are very different.
>> <http://www.net-security.org/news.php?id=610>

NETIQ DEVELOPS TOOLS TO KILL CAMERA/SHY
NetIQ announced that it had developed a tool to detect and disable the new anti-censorship application Camera/Shy.
>> <http://www.net-security.org/news.php?id=611>

HOUSE OKS LIFE SENTENCES FOR HACKERS
The House of Representatives overwhelmingly approved a bill that would allow for life prison sentences for malicious computer hackers.
>> <http://www.net-security.org/news.php?id=612>

CHINESE WEB PORTALS AGREE TO PURGE CRITICAL CONTENT
Internet portals in China, including Yahoo!'s Chinese-language site, have signed a voluntary pledge to purge the Web of content that China's communist government deems subversive.
>> <http://www.net-security.org/news.php?id=613>

MCAFEE SECURITY TO UPDATE LINE
McAfee Security will update its line of security products in August, including its antivirus and personal firewall software, as well as its system cleaning tool.
>> <http://www.net-security.org/news.php?id=614>

THE BEHAVIORS AND TOOLS OF TODAY'S HACKERS
The objectives of early hackers are a far cry from the goals of today's hacker. The motivation of the new breed of hackers appears not to be curiosity, or a hunger for knowledge, as it used to be.
>> <http://www.net-security.org/news.php?id=616>

CERT: SECURITY FLAW REPORTS INCREASING
The number of reported computer system security flaws has increased dramatically, according to CERT.
>> <http://www.net-security.org/news.php?id=617>

LIBERTY - IS USABILITY COMPATIBLE WITH SECURITY?
The Liberty 1.0 specification could make the Internet easier to use, but will it make it more or less safe?
>> <http://www.net-security.org/news.php?id=618>

IT SECURITY SPENDING DISAPPOINTS

Investors who had hoped that increased security concerns after Sept. 11 would yield an immediate bonanza in the information security sector have been sorely disappointed.

>> <http://www.net-security.org/news.php?id=619>

SECRET PASSWORD TO A HEADACHE

Consumers are suffering "password burnout" because they have to remember so many different codes and number combinations, according to a new report.

>> <http://www.net-security.org/news.php?id=620>

GOVERNMENT'S SEAL OF SECURITY

The federal government releases security standards and software it hopes individuals and businesses will adopt, along with government agencies, to configure systems against hackers.

>> <http://www.net-security.org/news.php?id=621>

SECURITY FILTER SPAWNS BIZARRE WORDS ON SITES

Hundreds of websites have been found to contain bizarre new words because an e-mail security filter used by Yahoo! has been actively changing them.

>> <http://www.net-security.org/news.php?id=622>

WI-FI HACKERS ARE STEALING BANDWIDTH

Time Warner has warned cable customers not to use their accounts to provide free internet access to others via wireless connectivity.

>> <http://www.net-security.org/news.php?id=623>

FEDS DEVISE CYBERSECURITY STANDARD

The Pentagon, the National Security Agency and private organizations have developed security standards for Windows 2000 in order to stop the most common assaults against federal networks.

>> <http://www.net-security.org/article.php?id=626>

STUDENT CHARGED WITH HACKING

A University of Delaware student broke into the school's computer system and gave herself passing grades in three courses, police said.

>> <http://www.net-security.org/news.php?id=627>

MICROSOFT PALLADIUM: ACCESS DENIED!

Microsoft has radical plans to install a 'gatekeeper' on personal computers, all in the name of security. But, asks Andy Goldberg, does this have grave implications for consumers?

>> <http://www.net-security.org/news.php?id=628>

MEET THE NIGERIAN E-MAIL GRIFTERS

Those increasingly ubiquitous Nigerian e-mails "respectfully requesting your assistance" and promising rewards actually do work - for the Nigerians. An admitted scammer explains how it works.

>> <http://www.net-security.org/news.php?id=629>

SYMANTEC BUYS THREE SECURITY FIRMS

Symantec said it has entered into deals to acquire three security firms - Recourse Technologies, Riptech and SecurityFocus - for a total of \$355 million in cash.

>> <http://www.net-security.org/news.php?id=630>

THWART ATTACKS FROM INSIDE THE WIRE

When security software vendor eEye had its Web site defaced, the company immediately suspected a "disgruntled employee." Most internal attackers, though, are stealthier.

>> <http://www.net-security.org/news.php?id=631>

HOME USERS PART OF NET SECURITY PLAN

Keeping your home computer's antivirus software updated is not just sensible – it could be a way to demonstrate your patriotism.

>> <http://www.net-security.org/news.php?id=632>

TEAM DEMOS 'FIRST QUANTUM CRYPTO PROTOTYPE MACHINE'

Boffins have moved one step closer to a practical implementation of the Holy Grail of encryption - quantum cryptography - by exchanging keys across a 67km fibre optic network.

>> <http://www.net-security.org/news.php?id=633>

SHARP RISE IN WEB SITE DEFAACEMENTS ON LINUX SERVERS

The number of defacements of Web sites on Linux-based systems recorded by London security consultancy mi2g Ltd. rose significantly in the first half of 2002.

>> <http://www.net-security.org/news.php?id=634>

SOUTH KOREAN HACKERS DECLARE WAR ON US

South Korean activists have declared cyber war on the US government following the involvement of US soldiers in the deaths of two teenage girls in a car crash.

>> <http://www.net-security.org/news.php?id=635>

THE DEVIL AND THE DEEP BLUE SEA

Why Microsoft's Palladium project threatens to send Linux and open-source into exile.

>> <http://www.net-security.org/news.php?id=636>

TECH ACTIVISTS PROTEST ANTI-COPYING

Enthusiasts of free software disrupted a Commerce Department meeting, insisting on their right to debate the entertainment industry over anti-copying technologies.

>> <http://www.net-security.org/news.php?id=637>

THE CASE OF THE MISSING CODE

If you were a terrorist schooled in fundamentalist Islam, mass violence, digital cryptography and the pack-rat ethos peculiar to eBay, in which corner of eBay site might you hide your plans for America's end?

>> <http://www.net-security.org/news.php?id=638>

FIRMS TACKLE CYBER-SABOTAGE

Cyber-sabotage is regarded as one of the business world's dirty little secrets. And it's one that is coming to light in the wake of scandals like Enron, Global Crossing and WorldCom.

>> <http://www.net-security.org/news.php?id=639>

STAR PHONE HACKER ARRESTED

A 34 year-old Hertfordshire man has been arrested over allegations that he hacked into the phone line of television presenter Angus Deayton. The man is thought to be a BT engineer.

>> <http://www.net-security.org/news.php?id=640>

JUSTIFYING THE EXPENSE OF IDS, PART ONE

This article will seek to demonstrate the value associated with a well thought out implementation and effective lifecycle management of IDS technology.

>> <http://www.net-security.org/news.php?id=641>

GATES SAYS MICROSOFT SECURITY PUSH COST \$100 MLN

Bill Gates said the company's campaign to improve the security of its software had cost at least \$100 million this year, but said the expense was paying off in better products.

>> <http://www.net-security.org/news.php?id=642>

HACKERS TRY A BANK JOB

A rival bank has been hacking into the website on which UBS Warburg stores information on derivatives trading for its staff and using this unauthorised information to assess their own market positions.

>> <http://www.net-security.org/news.php?id=643>

=====

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

Jigsaw Webserver DOS device Denial of Service Vulnerability
>> <http://www.net-security.org/vuln.php?id=1879>

Resin DOS Device Path Disclosure
>> <http://www.net-security.org/vuln.php?id=1878>

Macromedia Sitespring Cross Site Scripting Vulnerability
>> <http://www.net-security.org/vuln.php?id=1877>

Jigsaw Webserver Path Disclosure Vulnerability
>> <http://www.net-security.org/vuln.php?id=1876>

IBM Tivoli Management Framework Buffer Overflow
Vulnerability (Endpoint)
>> <http://www.net-security.org/vuln.php?id=1875>

ICQ and MSIE Allow Execution of Arbitrary Code
>> <http://www.net-security.org/vuln.php?id=1874>

Oddsock Playlist Generator Multiple Buffer Overflow Vulnerability
>> <http://www.net-security.org/vuln.php?id=1873>

Norton Personal Internet Firewall HTTP Proxy Vulnerability
>> <http://www.net-security.org/vuln.php?id=1872>

IBM Tivoli Management Framework Buffer Overflow
Vulnerability (ManagedNode)
>> <http://www.net-security.org/vuln.php?id=1871>

Novell Netmail Multiple Buffer Overflows
>> <http://www.net-security.org/vuln.php?id=1870>

Novell Netmail IMAP Service Multiple buffer Overflows
>> <http://www.net-security.org/vuln.php?id=1869>

Fluid Dynamics Search Engine Cross Site Scripting Vulnerability
>> <http://www.net-security.org/vuln.php?id=1868>

Sharp Zaurus SL-5000/D Multiple Vulnerabilities
>> <http://www.net-security.org/vuln.php?id=1867>

Cisco VPN3000 Gateway MTU Overflow Vulnerability
>> <http://www.net-security.org/vuln.php?id=1866>

SQL Server 7 & 2000 Installation and Service Packs
Write Encoded Passwords to a File
>> <http://www.net-security.org/vuln.php?id=1865>

MFC ISAPI Framework Buffer Overflow Vulnerability
>> <http://www.net-security.org/vuln.php?id=1864>

Adobe eBook Library Vulnerability
>> <http://www.net-security.org/vuln.php?id=1863>

IIS Microsoft SMTP Service Encapsulated SMTP Address Vulnerability
>> <http://www.net-security.org/vuln.php?id=1862>

Working Resources BadBlue Multiple Vulnerabilities
>> <http://www.net-security.org/vuln.php?id=1861>

Double Choco Latte Multiple Vulnerabilities
>> <http://www.net-security.org/vuln.php?id=1860>

[Advisories]

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

Conectiva Linux Security Advisory - libpng
>> <http://www.net-security.org/advisory.php?id=867>

Mandrake Linux Security Advisory - squid
>> <http://www.net-security.org/advisory.php?id=866>

Caldera Security Advisory - Linux: mod_ssl off-by-one error
>> <http://www.net-security.org/advisory.php?id=865>

Mandrake Linux Security Advisory - bind
>> <http://www.net-security.org/advisory.php?id=864>

Red Hat Security Advisory - Updated mod_ssl packages available
>> <http://www.net-security.org/advisory.php?id=863>

Conectiva Linux Security Advisory - instalador
>> <http://www.net-security.org/advisory.php?id=862>

Compaq Security Bulletin - HP Tru64 UNIX Potential inetd denial of service
>> <http://www.net-security.org/advisory.php?id=861>

Compaq Security Bulletin - HP Tru64 UNIX Potential Overflow in /usr/bin/ipcs
>> <http://www.net-security.org/advisory.php?id=860>

Caldera Security Advisory - OpenServer 5.0.5 OpenServer 5.0.6: uux status file name buffer overflow
>> <http://www.net-security.org/advisory.php?id=859>

Caldera Security Advisory - OpenServer 5.0.5 OpenServer 5.0.6: timed does not enforce nulls
>> <http://www.net-security.org/advisory.php?id=858>

FreeBSD Security Advisory - openssh contains remote vulnerability
>> <http://www.net-security.org/advisory.php?id=857>

Trustix Security Advisory - squid
>> <http://www.net-security.org/advisory.php?id=856>

Trustix Security Advisory - bind
>> <http://www.net-security.org/advisory.php?id=855>

Microsoft Security Bulletin MS02-035 - SQL Server Installation Process May Leave Passwords on System
>> <http://www.net-security.org/advisory.php?id=854>

Microsoft Security Bulletin MS02-034 - Cumulative Patch for SQL Server
>> <http://www.net-security.org/advisory.php?id=853>

SGI Security Advisory - Apache Web Server Chunk Handling vulnerability
>> <http://www.net-security.org/advisory.php?id=852>

FreeBSD Security Advisory - Users may trace previously privileged processes (ktrace module)
>> <http://www.net-security.org/advisory.php?id=851>

FreeBSD Security Advisory - Buffer overflow in tcpdump
when handling NFS packets
>> <http://www.net-security.org/advisory.php?id=850>

Caldera Security Advisory - UnixWare 7.1.1 Open UNIX 8.0.0:
rpc.ttdserverd file creation and deletion vulnerabilities
>> <http://www.net-security.org/advisory.php?id=849>

Conectiva Linux Security Advisory - Resolver libraries
>> <http://www.net-security.org/advisory.php?id=848>

[Virus News]

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

Beware of Frethem Worm
>> http://www.net-security.org/virus_news.php?id=51

Win32.Worm.Datom.A Analysis
>> http://www.net-security.org/virus_news.php?id=50

[Security world]

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

Symantec to Acquire Riptech
>> <http://www.net-security.org/press.php?id=907>

Symantec to Acquire Recourse Technologies
>> <http://www.net-security.org/press.php?id=906>

Symantec To Acquire SecurityFocus
>> <http://www.net-security.org/press.php?id=905>

GFI Launches EventLogScan, a Free Online Event Log Scanning Service
>> <http://www.net-security.org/press.php?id=904>

High Risk Of Spreading For The Frethem Virus
>> <http://www.net-security.org/press.php?id=903>

eOriginal Selects nCipher To Deliver Trustworthiness of Electronic Documents
>> <http://www.net-security.org/press.php?id=902>

Rainbow Technologies and SOFTBANK COMMERCE Team to Accelerate Deployment of iKey 1000 Security Token in PocketPC 2002 Environments
>> <http://www.net-security.org/press.php?id=901>

Datakey Expands Its Business With The Canadian Government
>> <http://www.net-security.org/press.php?id=900>

Norman And Fujitsu Siemens Increase The Standard Of Security On Home Computers
>> <http://www.net-security.org/press.php?id=899>

Datakey Announces Second Quarter Conference Call
>> <http://www.net-security.org/press.php?id=898>

Trusecure Announces Its Membership In The Microsoft Certified Partner Program
>> <http://www.net-security.org/press.php?id=897>

E-Mail Message "Your Password!" Is A Virus
>> <http://www.net-security.org/press.php?id=896>

High-spreading Virus Disguised as a Microsoft Update
>> <http://www.net-security.org/press.php?id=895>

[Featured articles]

All articles are located at:

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

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

Setuid Demystified

>> <http://www.net-security.org/article.php?id=151>

More Enforceable Security Policies

>> <http://www.net-security.org/article.php?id=150>

Linux Security Modules: General Security Support for the Linux Kernel

>> <http://www.net-security.org/article.php?id=149>

[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

SQL SERVER PASSWORD AUDITING TOOL 1.0.0

This tool should be used to audit the strength of Microsoft SQL Server passwords offline. The tool can be used either in BruteForce mode or in Dictionary attack mode.

>> <http://www.net-security.org/software.php?id=200>

ANTI DATOM

This is a removal tool for Win32.Worm.Datom, which is a new network worm that uses shared folders in the local network to spread itself.

>> <http://www.net-security.org/software.php?id=201>

FWANALOG 0.6.1

fwanalog is a shell script that parses and summarizes firewall logfiles. It currently understands logs from ipf (tested with OpenBSD 2.8's and 2.9's ipf, also FreeBSD, NetBSD and Solaris 8 with ipf), OpenBSD 3.0 pf, Linux 2.2 ipchains, Linux 2.4 iptables and some ZyXEL/NetGear routers.

>> <http://www.net-security.org/software.php?id=202>

GNUZZA 0.4.2

This is a small peer-to-peer chat with some extra features. It uses Diffie-Hellmann key agreement, with variable bit primes (1024-4096), to exchange sessions keys and these keys are used to encrypt each byte that is sent or received.

>> <http://www.net-security.org/software.php?id=203>

GUARDDOG 2.0.0

Guarddog is a firewall configuration utility for Linux systems. Guarddog is aimed at two groups of users. Novice to intermediate users who are not experts in TCP/IP networking and security, and those users who don't want the hassle of dealing with cryptic shell scripts and ipchains/iptables parameters.

>> <http://www.net-security.org/software.php?id=204>

VCATCH 5.0

VCatch is a virus protection software. When VCatch is active it will check all the files sent or downloaded to your computer via Email and Web applications. In the event that VCatch detects that a file is suspected to be a virus, the software automatically deletes the file and notifies you.

>> <http://www.net-security.org/software.php?id=205>

ANTI FRETHEM

This is a removal tool for Frethem worm. The e-mail message carries only one subject field: "Re: Your password!" and exploits the vulnerability in Microsoft Internet Explorer versions 5.01 and 5.5.

<http://www.net-security.org/software.php?id=206>

CYBERSCRUB

CyberScrub is a high level military grade security application designed to help you completely eliminate sensitive information from your computer, protect your Internet privacy, and enhance system performance.

>> <http://www.net-security.org/software.php?id=207>

GRSECURITY 1.9.5

grsecurity is a complete security system for Linux 2.4 that implements a detection/prevention/containment strategy.

>> <http://www.net-security.org/software.php?id=208>

RCF 5.2.1S1

rcf (aka rc.firewall) is an ipchains-based firewall with support for over 50 network service modules (including vtun, dhcp, nfs, smb, napster, proxies, online games, etc.), masquerading, port forwarding, and ip accounting.

>> <http://www.net-security.org/software.php?id=209>

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