



Newsletter
Issue 130

Issue 130 - 04.10.2002

<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>.

***** ALERT! *****

ALL OF THE FOLLOWING APPLICATIONS ARE VULNERABLE TO ATTACK!:

- *** Oracle
- *** Microsoft SQL Server
- *** Sybase
- *** Lotus Domino

QUESTION: How Vulnerable are Your Applications?

ANSWER: Find out by downloading AppDetective from:

***** <http://www.appsecinc.com/products/#pentest>

AppDetective will DISCOVER Rogue Installations; Perform Zero Knowledge PENETRATION TESTS without Administrative Rights; and Perform In-Depth SECURITY AUDITS from the Inside-Out without Agents.

DOWNLOAD YOUR FREE EVALUATION VERSION TODAY FROM:

<http://www.appsecinc.com/products/#pentest>

Table of contents:

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

[**General security news**]

THE "PRIVACY2002" GATHERING IN CLEVELAND

Privacy and security experts gathered this week to network and share their fears about the threat ever-evolving technology poses to ordinary consumers, business and governments alike.

>> <http://www.net-security.org/news.php?id=1127>

HACKER GROUPS DECLARE WAR ON US.GOV

A record number of malicious hacking attempts were made this month, and anti-American groups are responsible.

>> <http://www.net-security.org/news.php?id=1128>

VIRUSES ARE DEAD. LONG LIVE VIRUSES!

This year has been mercifully quiet on the virus front but anyone who reckons the virus problem has finally been beaten is failing to learn the lessons of history.

>> <http://www.net-security.org/news.php?id=1129>

EMAIL ON SOHO NETWORKS

In this article, Jeffrey L. Taylor provides detailed steps for implementing your own email system.

>> <http://www.net-security.org/news.php?id=1130>

PORN SPAM: IT'S GETTING RAUNCHIER

Disturbing, explicit and sometimes-illegal pornographic images are popping up unsolicited in e-mail boxes everywhere.

>> <http://www.net-security.org/news.php?id=1131>

NEW NET PROJECT AIMS TO AVOID HACKING

Scientists concerned about the vulnerability of the Internet to failure or hacking envision a next-generation system that would use the collective power of users' computers to become more secure.

>> <http://www.net-security.org/news.php?id=1132>

AGENCY PROBES D.C. WIRELESS NETWORK

Secret Service agents are using a laptop and an antenna fashioned from a Pringles potato chip can while looking for security holes in wireless networks in Washington.

>> <http://www.net-security.org/news.php?id=1133>

ONLINE PAYMENT SERVICE PAYPAL HIT BY SCAM

PayPal officials acknowledged the company has been the target of a scam designed to get users' personal information. But it hasn't warned customers to be wary.

>> <http://www.net-security.org/news.php?id=1134>

WINTASKS PROCESS LIBRARY

The newly opened WinTasks Process Library contains information about all common Windows processes as is continuously updated with new information.

>> <http://www.net-security.org/news.php?id=1135>

EBUSINESS U.S. TECH PROTESTS EU PRIVACY LAWS

A group of American companies is attempting this week to persuade the European Union to relax its rules governing data protection, claiming they are bad for business.

>> <http://www.net-security.org/news.php?id=1137>

GSA TO UNVEIL TOP 20 SECURITY FLAWS, FOCUS ON FIXE

The focus will be on fixes this week when the U.S. General Services Administration unveils its list of the top 20 Internet security vulnerabilities to a gathering of about 350 IT professionals.

>> <http://www.net-security.org/news.php?id=1138>

HONEYMOON OVER FOR LINUX USERS

Iain Thomson writes: "As open source software becomes increasingly popular it is being targeted by virus writers and proving to be at least as vulnerable as Microsoft."

>> <http://www.net-security.org/news.php?id=1139>

INSIDERS, NOT HACKERS, BIGGEST INFORMATION THEFT RISK

U.S. companies worried about hackers stealing their trade secrets should be even more afraid of former employees, competitors and contractors, according to a new study.

>> <http://www.net-security.org/news.php?id=1140>

WEB SITE DEFAACEMENTS HIT ALL-TIME HIGH

More than 9000 attacks were recorded in September, with U.S. sites the prime targets, researcher says.

>> <http://www.net-security.org/news.php?id=1141>

FBI TO RELEASE COMPUTER-SECURITY UPDATES

The FBI and SANS have a new initiatives to keep companies up to date on the most threatening software vulnerabilities.

>> <http://www.net-security.org/news.php?id=1142>

SPAM FILTERING TECHNIQUES

In this article, David discusses and compares several broad approaches to the automatic elimination of unwanted e-mail while introducing and testing some popular tools that follow these approaches.

>> <http://www.net-security.org/news.php?id=1143>

ONE PATCH TO RULE THEM ALL

A recent XP security hole begs the question, do we really want Microsoft to release individual fixes for every bug?

>> <http://www.net-security.org/news.php?id=1144>

UNIX TOOLS TRACE HACKERS

If you find you've been cracked use these old-school Unix tools to help track down the perpetrators.

>> <http://www.net-security.org/news.php?id=1145>

WHO'S LISTENING IN ON YOUR MESSAGES?

Too many organizations have critical data sitting on unsecured enterprise networks. Illena Armstrong explains how encryption technologies can protect this major asset.

>> <http://www.net-security.org/news.php?id=1147>

'BUGBEAR' WORM OPENS BACKDOORS

Anti-virus companies warned computer users about a new worm that opens up a backdoor in the computers and logs keystrokes.

>> <http://www.net-security.org/news.php?id=1148>

BOOK REVIEW: XML SECURITY BOOKS

XML was originally developed without any thought to security and privacy. Here are reviews of two XML security books.

>> <http://www.net-security.org/news.php?id=1149>

SECURITY AGENCY INCREASES MONITORING

The NSA spent \$282 million to upgrade the technology it uses to sift through the huge volume of telephone conversations, e-mail and other worldwide communications chatter it monitors.

>> <http://www.net-security.org/news.php?id=1150>

EXAMINING THE CIW SECURITY PROFESSIONAL EXAM

The CIW Security Professional exam requires knowledge of basic security concepts as well as how they are implemented in Linux/Unix and Windows NT/2000 servers.

>> <http://www.net-security.org/news.php?id=1151>

PRO-ISLAMIC MILITANT HACKER GROUPS BOOST ATTACKS

Pro-Islamic hacker group Unix Security Guards increased its activity tenfold to highlight the Palestinian cause and show solidarity with the Arab world as tensions rise in regard to the US conflict with Iraq.

>> <http://www.net-security.org/news.php?id=1152>

CAN SOFTWARE SECURITY BE CERTIFIED?

New rules for encryption products sold to Uncle Sam tighten the acceptable standards. That's a good start toward a worthy goal.

>> <http://www.net-security.org/news.php?id=1153>

SCAN OF THE MONTH - A NEW CHALLENGE

This month's challenge is very different. Your job is to recover and analyze a floppy from a suspected drug dealer.

>> <http://www.net-security.org/news.php?id=1154>

THE NEW FACE OF MALICIOUS CODE

The profile of malicious code on the Internet is changing with diallers and Trojan horses becoming more serious problems.

>> <http://www.net-security.org/news.php?id=1155>

GARTNER SLAMS MS SECURITY AFTER LATEST FLAW

The latest flaw with a major Microsoft product shows Redmond is unlikely to have anything that approximates to secure software until 2004 at the earliest.

>> <http://www.net-security.org/news.php?id=1156>

SKT DENIES ALLEGATIONS OF WIRETAPPING

SK Telecom, Korea's largest mobile communications service provider, has flatly denied allegations that it is virtually impossible to listen in to calls on the 011 network.

>> <http://www.net-security.org/news.php?id=1157>

IT'S A BUG, A BEAR AND A WORM

Watch out for Bugbear, the latest malicious worm making the rounds. Antiviral companies are naturally apoplectic over it because it is one of the nastiest ones to date.

>> <http://www.net-security.org/news.php?id=1158>

NIGERIAN EMAIL SCAM BROKEN UP

Spanish police have smashed a Nigerian-led scam that reaped up to €20 million.

>> <http://www.net-security.org/news.php?id=1159>

RSA DEBUTS XML SIGNATURES SECURITY FOR WEB

RSA Security has begun shipping its software development kit, RSA BSAFE SecurXML-C, allowing developers to add digital signatures using XML technology to Web services.

>> <http://www.net-security.org/news.php?id=1160>

PORT 137 SCANS

As a followup to a Incidents mailing list thread on port 137 scans, ISC believes that the increase of these scans is connected to Bugbear and Scrup worms.

>> <http://www.net-security.org/news.php?id=1161>

KEVIN MITNICK HAWKING HISTORIC LAPTOPS, BOOK

Famed hacker Kevin Mitnick said he is coming clean and hoping to make some money in the process.

>> <http://www.net-security.org/news.php?id=1162>

WIRELESS MESH AND AD-HOC TECHNOLOGIES

Aashih Patil has mulled over the potential of various wireless technologies, and thinks that ad-hoc and mesh networks are worth talking about right now.

>> <http://www.net-security.org/news.php?id=1163>

SLAPPERII.A AKA SLAPPER.D VARIANT

The SlapperII.A variant was first detected on or around 28 September 2002. This worm retrieves the majority of its payload from a web server and also acts as an IRCbot.

>> <http://www.net-security.org/news.php?id=1164>

SANS AND FBI TOP 20 VULN LIST

SANS and FBI have announced the 20 most serious security vulnerabilities affecting both Windows and Unix systems.

>> <http://www.net-security.org/news.php?id=1165>

NEWS REPORT: SATELLITES AT RISK OF HACKS

Want to find the most-ignored cybersecurity hole in America's critical infrastructure? Congressional investigators say, Look up!

>> <http://www.net-security.org/news.php?id=1166>

US GOVERNMENT SITE HACKED

The US State Department briefly shut down one of its websites this week after computer hackers defaced its homepage with obscenities.

>> <http://www.net-security.org/news.php?id=1167>

THE BOOK ON MITNICK IS BY MITNICK

The social-engineering hacker whose name is synonymous with computer fraud has a new book and a nearly new lease on life.

>> <http://www.net-security.org/news.php?id=1168>

SCIENTISTS FIND KEY TO WATER-TIGHT ENCRYPTION

Researchers have managed to send untamperable encryption keys over long distances, opening the way for secure communications.

>> <http://www.net-security.org/news.php?id=1169>

SECURITY BENCHMARK TOOLS AVAILABLE

All federal agencies can now freely distribute and use the security configuration tools developed by the independent Center for Internet Security and endorsed by federal security experts.

>> <http://www.net-security.org/news.php?id=1170>

INHOSPITABLE HOSTS

Mike Bobbitt writes: "Attackers may try the door, but intrusion prevention tools won't let them in."

>> <http://www.net-security.org/news.php?id=1171>

SECURITY: THE NUMBER ONE WORRY FOR IT PROS

A study claims to identify the pressures faced by IT managers and IT Directors in European companies with more than 200 employees. Guess what most of these people are worried about: Security.

>> <http://www.net-security.org/news.php?id=1172>

6 MYTHS ABOUT SECURITY POLICIES

Al Berg writes: "In the course of working on the new policies, I learned the truth about my assumptions, which I now call the "Six Myths of Infosecurity Policies."

>> <http://www.net-security.org/news.php?id=1173>

FEDERAL PROPOSAL TELLS ONLY PART OF CYBERCRIME STORY

In the wake of the Sept. 11 terrorist attacks, the Canadian government hurriedly introduced a series of new anti-terror measures...

>> <http://www.net-security.org/news.php?id=1174>

HNS COVERAGE FROM RSA CONFERENCE 2002 EUROPE

The Help Net Security staff will attend the conference and all the appropriate exhibitions and classes. Be sure to expect all the scoops, photos and interviews from the conference.

The coverage from the conference is sponsored by ScannerX - <http://www.scannerx.com/free1.htm>

[Vulnerabilities]

All vulnerabilities are located here:
http://www.net-security.org/archive_vuln.php

Buffer Overflow in Internet Explorer/Outlook HTML Help
>> <http://www.net-security.org/vuln.php?id=2098>

Apache 2.0 Cross-Site Scripting Vulnerability
>> <http://www.net-security.org/vuln.php?id=2097>

Carello 1.3 Remote File Execution Vulnerability Addendum
>> <http://www.net-security.org/vuln.php?id=2096>

TightAuction, PY-Membres, upb PB, MidiCart PHP and PPhlogger Vulnerabilities
>> <http://www.net-security.org/vuln.php?id=2095>

Net-SNMP Denial of Service Vulnerability
>> <http://www.net-security.org/vuln.php?id=2094>

phpWebSite Cross Site Scripting Vulnerability
>> <http://www.net-security.org/vuln.php?id=2093>

Crashing Unisys Clearpath with nmap
>> <http://www.net-security.org/vuln.php?id=2092>

MySQL Windows Version Locally Exploitable Buffer Overflow Vulnerability
>> <http://www.net-security.org/vuln.php?id=2091>

Jetty CGIServlet Arbitrary Command Execution Vulnerability
>> <http://www.net-security.org/vuln.php?id=2090>

Compaq Insight Manager Http Server Cross Site Scripting Vulnerability
>> <http://www.net-security.org/vuln.php?id=2089>

NetGear FVS318 Firewall Router Firmware 1.1 Username/Password
Disclosure Vulnerability
>> <http://www.net-security.org/vuln.php?id=2088>

Zope Versions pre 2.5.1b2 Reveal Complete Physical Location
>> <http://www.net-security.org/vuln.php?id=2087>

WN Server Buffer Overflow Vulnerability
>> <http://www.net-security.org/vuln.php?id=2086>

SunONE Starter Kit v2.0 SearchDisk Vulnerability
>> <http://www.net-security.org/vuln.php?id=2085>

Fetchmail Remote Vulnerabilities
>> <http://www.net-security.org/vuln.php?id=2084>

Monkey HTTP Server Cross Site Scripting Vulnerabilities
>> <http://www.net-security.org/vuln.php?id=2083>

Watchguard Firewall Appliances Security Issues
>> <http://www.net-security.org/vuln.php?id=2082>

Jetty jsp/servlet Engine Cross Site Scripting Vulnerability
>> <http://www.net-security.org/vuln.php?id=2081>

Multiple Vulnerabilities in WASD http Server for OpenVMS
>> <http://www.net-security.org/vuln.php?id=2080>

[**Advisories**]

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

Gentoo Linux Security Announcement - python
>> <http://www.net-security.org/advisory.php?id=1090>

Gentoo Linux Security Announcement - gv
>> <http://www.net-security.org/advisory.php?id=1089>

EnGarde Secure Linux Advisory - tar: directory traversal vulnerability

>> <http://www.net-security.org/advisory.php?id=1088>

Microsoft Security Bulletin MS02-057 - Flaw in Services for Unix 3.0 Interix SDK Could Allow Code Execution

>> <http://www.net-security.org/advisory.php?id=1087>

Microsoft Security Bulletin MS02-056 - Cumulative Patch for SQL Server

>> <http://www.net-security.org/advisory.php?id=1086>

Microsoft Security Bulletin MS02-055 - Unchecked Buffer in Windows Help Facility Could Enable Code Execution

>> <http://www.net-security.org/advisory.php?id=1085>

Microsoft Security Bulletin MS02-054 - Unchecked Buffer in File Decompression Functions Could Lead to Code Execution

>> <http://www.net-security.org/advisory.php?id=1084>

Conectiva Linux Security Announcement - XFree86

>> <http://www.net-security.org/advisory.php?id=1083>

EnGarde Secure Linux Advisory - fetchmail-ssl: buffer overflows and broken boundary checks

>> <http://www.net-security.org/advisory.php?id=1082>

EnGarde Secure Linux Advisory - glibc: several security-related updates

>> <http://www.net-security.org/advisory.php?id=1081>

Conectiva Linux Security Announcement - python

>> <http://www.net-security.org/advisory.php?id=1080>

Gentoo Linux Security Announcement - unzip

>> <http://www.net-security.org/advisory.php?id=1079>

Compaq Security Bulletin - HP OpenVMS Potential POP server local vulnerability

>> <http://www.net-security.org/advisory.php?id=1078>

Gentoo Linux Security Announcement - fetchmail

>> <http://www.net-security.org/advisory.php?id=1077>

Gentoo Linux Security Announcement - tar

>> <http://www.net-security.org/advisory.php?id=1076>

SuSE Security Announcement - heimdal
>> <http://www.net-security.org/advisory.php?id=1075>

Red Hat Security Advisory - Updated unzip and tar packages
fix vulnerabilities
>> <http://www.net-security.org/advisory.php?id=1074>

Gentoo Linux Security Announcement - glibc (update)
>> <http://www.net-security.org/advisory.php?id=1073>

Gentoo Linux Security Announcement - dietlibc
>> <http://www.net-security.org/advisory.php?id=1072>

[**Featured articles**]

All articles are located at:
http://www.net-security.org/articles_main.php

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

INTERVIEW WITH RODERICK W. SMITH
Roderick W. Smith is a professional computer book author who has extensive experience writing handbooks for users. A Linux and networking expert, he has several books to his name.
>> <http://www.net-security.org/article.php?id=194>

INTERVIEW WITH JON CALLAS
Jon Callas, one of the founders of the new PGP Corporation, is an innovator and an acknowledged expert in all major aspects of contemporary business security.
>> <http://www.net-security.org/article.php?id=195>

[**Security world**]

All press releases are located at:

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

Entercept Security Technologies Announces Integration Plans with
the Symantec Security Management System

>> <http://www.net-security.org/press.php?id=1042>

Check Point Software Technologies Ltd. Achieves Q3 Targets

>> <http://www.net-security.org/press.php?id=1041>

Baltimore Introduces New Security Toolkit for Web Services
Environments

>> <http://www.net-security.org/press.php?id=1040>

Bugbear Climbs to Second Place in The List of Most Frequently
Detected Viruses by ActiveScan

>> <http://www.net-security.org/press.php?id=1039>

Complete Suite of WLAN Security Solutions Launched

>> <http://www.net-security.org/press.php?id=1038>

Snapgear Safe From Microsoft PPTP Vulnerability

>> <http://www.net-security.org/press.php?id=1037>

Protegrity And nCipher Announce New Database Security
Software Intregrated With Fips 140 Validated Hardware

>> <http://www.net-security.org/press.php?id=1036>

Hacker Attacks Possible as E-mail Worm Disables Antivirus
Programs and Firewalls

>> <http://www.net-security.org/press.php?id=1035>

SSH Communications Security Corp Partners With nCipher To Ensure
Enterprises And Service Providers Safe Storage Of Private Keys

>> <http://www.net-security.org/press.php?id=1034>

Kyberpass Launches Next Generation TrustPlatform

>> <http://www.net-security.org/press.php?id=1033>

Datakey Smart Card Technology Deployed by U.S. Government Agency

>> <http://www.net-security.org/press.php?id=1032>

Hurwitz Group Calls TruSecure "A Holistic Approach To Security"
>> <http://www.net-security.org/press.php?id=1031>

Highlights of Utimaco Safeware for the ISSE 2002
(October 2-4, 2002, Paris)
>> <http://www.net-security.org/press.php?id=1030>

[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

GNUPG 1.2.0

GnuPG stands for GNU Privacy Guard and is GNU's tool for secure communication and data storage. It can be used to encrypt data and to create digital signatures.
>> <http://www.net-security.org/software.php?id=295>

SPAMPAL 1.06

SpamPal sits between your email program and your mailbox, checking your email as you retrieve it.
>> <http://www.net-security.org/software.php?id=295>

SYSTEM SHIELD 2.0

System Shield prevents recovery of private or confidential information on your computer by securely overwriting the data. It uses methods approved by the US Department of Defense and other military agencies to ensure that data you wish to be deleted is permanently removed, no matter what technique of recovery is attempted.
>> <http://www.net-security.org/software.php?id=297>

MEGAPING 3.8

MegaPing is a set of diagnostics and information tools. It brings the convenience of Windows to the most commonly used internet utilities, including DNS lookup name, DNS list hosts, Finger, Host Monitor, IP scanner, NetBIOS scanner, Network time synchronizer, Ping, Port scanner, Share Scanner, Traceroute, and Whois.
>> <http://www.net-security.org/software.php?id=298>

SMARTWHOIS 3.5

SmartWhois is a useful network information utility that allows you

to find all the available information about an IP address, hostname, or domain, including country, state or province, city, name of the network provider, administrator and technical support contact information.

>> <http://www.net-security.org/software.php?id=299>

MULTINETWORK MANAGER 6.3

Do you connect to more than one network? Tired of reconfiguring your computer for every new location?

- With the MultiNetwork Manager (mnm) boot application, you can select a configuration already at boot time. mnm is developed to assist users working in "Dynamic Networking Environments".

- It provides an easy-to-navigate-tabbed dialog window that is used to connect your computer to different networks (e.g. ISPs or LANs) or multihome environments.

>> <http://www.net-security.org/software.php?id=300>

SUPER WEBSCAN 8.0

Super Webscan is a tool for network administrators that allows to detect open relay SMTP servers.

>> <http://www.net-security.org/software.php?id=301>

BITDEFENDER ANTI BUGBEAR

This tool removes Win32.BugBear.A@mm, an Internet worm that is spreading through e-mail. The worm uses the iframe exploit and it will execute itself on preview on some computers with older variants of Internet Explorer.

>> <http://www.net-security.org/software.php?id=302>

SOPHOS ANTI BUGBEAR-A

W32/Bugbear-A exploits a security loophole in some versions of Microsoft Outlook. Microsoft issued a patch which reportedly fixes this loophole last year, but some users have still not patched against it. For this reason the worm appears to be particularly infecting home users who are sometimes less security conscious.

>> <http://www.net-security.org/software.php?id=303>

NETWORKACTIV SNIFFER 1.4.2.2

NetworkActiv Sniffer is a TCP/IP packet sniffer with an easy to use interface.

>> <http://www.net-security.org/software.php?id=304>

[**Virus News**]

All virus news are located at:

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

Protecting Your Computer from Opasoft Worm

>> http://www.net-security.org/virus_news.php?id=96

Central Command: Top 12 Viruses For September 2002

>> http://www.net-security.org/virus_news.php?id=95

Bugbear Removal Tools

>> http://www.net-security.org/virus_news.php?id=94

Bugbear Worm Spreading at an Alarming Rate

>> http://www.net-security.org/virus_news.php?id=93

Kaspersky Labs: Virus Top 20 for September 2002

>> http://www.net-security.org/virus_news.php?id=92

Sophos: Top 10 Viruses and Hoaxes in September 2002

>> http://www.net-security.org/virus_news.php?id=91

Tanatos - A Worm with a "Trojan" In Its Pocket

>> http://www.net-security.org/virus_news.php?id=90

Panda Software Warns on New Worm Opaserv

>> http://www.net-security.org/virus_news.php?id=89

Sophos Suggestions for Taking Care of Bugbear

>> http://www.net-security.org/virus_news.php?id=88

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