

Net-Sec newsletter  
Issue 35 - 23.10.2000  
<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://www.net-security.org>.

Subscribe to this weekly digest on:  
<http://www.net-security.org/text/newsletter>

Table of contents:

- 1) General security news
- 2) Security issues
- 3) Security world
- 4) Featured articles
- 5) Featured books
- 6) Security software
- 7) Defaced archives

=====  
In association with Kaspersky Lab ([www.kaspersky.com](http://www.kaspersky.com)), HNS staff created a new section of the site, with about 400 descriptions of well known and not so know viruses. Specially interesting part of that section are screenshots of 50 virus infections. All viruses are well categorized and easy to browse.

Point your browser to this URL:  
<http://www.net-security.org/text/viruses>  
=====

#### General security news

-----

-----

#### FEDS' SECURITY ROLE MAY YIELD BUSINESS BENEFITS

Garnering low marks on IT security efforts and realizing that many of the nation's most sensitive networks are now situated in the private sector, the federal government more than ever is drumming up security-related partnerships with Corporate America.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.infoworld.com/articles/hn/xml/00/10/16/001016hnnist.xml>

#### DNS SECURITY UPGRADE PROMISES A SAFER 'NET

An emerging technology promises to improve the security of the Internet's infrastructure by preventing hackers from hijacking Web traffic and redirecting it to bogus sites. The new security mechanism, dubbed DNSSEC, plugs a hole in the Internet's Domain Name System that attackers have exploited to spoof

Web sites. DNSSEC prevents these attacks by allowing Web sites to verify their domain names and corresponding IP addresses using digital signatures and public-key encryption.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.nwffusion.com/news/2000/1016dnsec.html>

#### ABNORMAL IP PACKETS

This article, a discussion of the characteristics of abnormal Internet Protocol packets, is the first in a series of tutorials that are intended to educate intrusion detection system administrators about IP. As the use of network intrusion detection systems becomes more widespread, system administrators must learn how to use them effectively. Unfortunately, many admins do not have a thorough knowledge of IP. So even though an IDS may produce alerts about particular scans and attacks, an admin may not understand what the alerts mean.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.securityfocus.com/focus/ids/articles/abnormal1.html>

#### BSDCON'S BSD SYSTEM SECURITY TUTORIAL

"This year's BSDCon is being held at the Monterey Hyatt, in Monterey Ca. The first tutorial was a two-day tutorial covering BSD System Security. For the most part the classes are intensive and there was a lot of ground to cover. And attendees should have been fairly comfortable with at least one flavor of UNIX. However there was considerable mention of routers and their important role in overall network security."

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.bsdtoday.com/2000/October/News311.html>

#### SPAMMERS

ClickAction Inc. today said it was working with the FBI and several Internet service providers to determine the source of a series of "spam" attacks, wherein millions of bogus political campaign e-mail messages were sent via hijacked third party servers. The company said the messages, sent via numerous third-party ISP servers, include references to a ClickAction hosted Web site.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.computeruser.com/news/00/10/16/news4.html>

#### SUMMERCON RFP

The oldest of the living security/hacker conferences Summercon 2001 will be hosted in the Dutch city of Amsterdam at the Grand Hotel Krasnapolsky. Summercon 2001 will be broadcasted live via streaming media and presentations, with additional content, and collateral will be edited for future download from the website. You could submit your paper until 30 November 2000.

Link: <http://www.summercon.org/>

#### COMPUTER INTRUSION CASES

Here is a summary chart of recently prosecuted computer cases. This listing is a representative sample; it is not exhaustive. You can click on the name of the case to read a press release about the case.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://cybercrime.gov/cccases.html>

#### HV2K MEMBER INDICTED

18-year-old Robert Russell Sanford, member of hv2k, suspected of defacing government web sites in Texas and Canada last winter, surrendered to Dallas County authorities last Friday, a day after he was indicted on charges for defacing.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://web.lexis-nexis.com/more/cahners-chicago/11407/6439100/6>

#### SUIDNET - AN ONGOING SOLUTION

"I come not to bury Suidnet, but to praise it. Well, that is not entirely true, there are still some significant problems with Suidnet, but it looks to be the start of something good. I wouldn't be surprised if you haven't heard of Suidnet. It's an effort by IRC and security enthusiasts to create a more secure IRC network."

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://securityportal.com/closet/closet20001018.html>

#### BUG-HUNTERS SAY FIRMS IGNORING SECURITY HOLES

Major software firms may be neglecting security vulnerabilities and putting their users at serious risk, according to bug-hunters at Swedish security firm Defcom. The group says the situation has forced it to consider publicising the details of several exploits which would cause the companies involved embarrassment. Although Defcom says the majority of firms respond quickly to alerts, it claims that at least two large firms have failed to get back to it over a number of months. It is now holding last minute discussions with the firms, but says it is still considering releasing details.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.zdnet.co.uk/news/2000/41/ns-18519.html>

#### DON'T JUST COMPLAIN ABOUT SECURITY

Federal agencies must work more closely with industry to get government security needs built into products as they are developed, rather than going to vendors for fixes after the fact, according to public and private-sector experts.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.fcw.com/fcw/articles/2000/1016/web-nissc-10-17-00.asp>

#### INSIDEDDEFENSE - SPECIAL REPORT

A year after two teams of experts concluded the National Security Agency was suffering from profound operational and organizational problems, the director of the Ft. Meade, MD-based signals intelligence organization said last week he is beginning to see the initial benefits of a sweeping transformation effort aimed at changing the agency's culture, improving its technical capabilities and repairing its relationships with key stakeholders.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://cryptome.org/nsa-reorg-id.htm>

#### WEB ANONYMITY UNDER SIEGE

A Florida appeals court ruled that ISPs can be compelled by subpoena to identify people who post defamatory messages on Internet bulletin boards, even when the libellous nature of the statements has yet to be proved. In this case, Hvide Marine company former CEO Erik Hvide was seeking the identities of eight people who criticised both him and his company on a BBS. The subpoena had been

temporarily blocked pending appeal, and the appellate court chose to let it proceed.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.theregister.co.uk/content/1/14060.html>

#### EARTHLINK FLAW EXPOSES DOMAINS

A one-two punch of poor security left up to 81,000 domains hosted by Internet service provider EarthLink Inc. open to defacement and exploitation for at least a week. The vulnerability resulted from a recently discovered flaw in an open-source e-commerce package combined with a misconfigured hosting server operated by EarthLink subsidiary MindSpring.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.zdnet.com/zdnn/stories/news/0,4586,2641790,00.html>

#### ACER NOTEBOOK SUPPORTS SECURITY CARDS, WIRELESS

Acer's new TravelMate 350 notebook is barely an inch thick and weighs just 4 pounds, but it's chock full of new technology. The unit includes a built-in smart card reader and the hardware to add integrated Bluetooth wireless connectivity.

Link: [http://www.net-security.org/cgi-bin/news.cgi?url=http://www.idg.net/ic\\_273308\\_1794\\_9-10000.html](http://www.net-security.org/cgi-bin/news.cgi?url=http://www.idg.net/ic_273308_1794_9-10000.html)

#### SECURITY TESTS FOR EMPLOYEES

At the National Security Agency, the U.S. government's secretive intelligence gathering arm, employees are required to pass a test to show basic understanding of information security policy and procedures. Failing the test may result in a loss of an e-mail account and system access rights. It's no idle threat, says U.S. Air Force Col. John Whiteford, the deputy CIO at the NSA. All employees - from the agency's director on down - must complete the Web-based information security training course, which is followed by a 25- to 30-question, multiple-choice online test. If they fail, they take it again. So far, no one has lost his access rights, said Whiteford.

Link: [http://www.net-security.org/cgi-bin/news.cgi?url=http://www.idg.net/ic\\_273442\\_1794\\_9-10000.html](http://www.net-security.org/cgi-bin/news.cgi?url=http://www.idg.net/ic_273442_1794_9-10000.html)

#### ANTI-HACKING SQUADS COULD HELP CORPORATES

Gartner has called on enterprises to consider establishing specialist internal anti-hacking teams who would have wide ranging powers to defend against internet attacks. William Spernow, Gartner research director, said that such a team would realistically cost \$250,000 a year to run, and would be hard to sell to chief executives, but was needed in order to defend technology infrastructures.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.vnunet.com/News/1112675>

#### THE THROWAWAY CREDIT CARD

Following American Express's launch of a similar product last month, MBNA, the world's largest independent credit card issuer, announced plans to give consumers a more secure way of shopping online, with a disposable credit card number. MBNA will use technology created by New York-based Orbiscom to allow its 45 million Visa and MasterCard customers to buy goods on the Net without ever disclosing their personal credit card number.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.thestandard.com/article/display/0,1151,19505,00.html>

#### WORKING THE BIG COMPUTER CRIME CASE

Crimes may be geographically diverse, crossing state, national, and international boundaries. They may involve multiple networks and domains. In cases of fraud, investigative and analytical methods have to fit individuals from diverse localities into a larger picture or pattern.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://securityportal.com/articles/crime20001019.html>

#### COMPUTER CRIME TREATY THREATENS HUMAN RIGHTS

An international coalition of 28 human rights and civil liberties groups has called on the Council of Europe to alter its draft treaty on International cybercrime, warning that the agreement could violate the European Convention on Human Rights and rob Internet users of their freedom. The Global Internet Liberty Campaign (GILC) attacks draft proposals to increase the power given to law enforcers to intercept international communications and traffic data as part of their investigations. The group says such measures would give police forces free range to wiretap Internet users and would be open to abuse.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.zdnet.co.uk/news/2000/41/ns-18546.html>

#### MAVERICK JOINS ARMY FOR NETWORK SECURITY

The Army will use a new product from General Dynamics Electronic Systems for testing network vulnerabilities and for training soldiers to respond to cyberattacks. The company bills the product named Maverick as "the first commercially available Internet security software to combine Internet reconnaissance and Internet attack capabilities."

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.fcw.com/fcw/articles/2000/1016/web-infowar-10-19-00.asp>

#### DENIAL-OF-SERVICE ATTACKS STILL A BIG THREAT

The types of massive distributed denial-of-service attacks that knocked several big e-commerce Web sites out of action earlier this year remain a viable threat that could grow even more sophisticated, according to experts at this week's government-sponsored National Information Systems Security Conference. Experts at the conference - which was sponsored by the National Institute of Standards and Technology and the National Security Agency's National Computer Security Center - said there currently are no adequate mechanisms for stopping DDOS attacks.

Link: [http://www.net-security.org/cgi-bin/news.cgi?url=http://www.idg.net/ic\\_274724\\_1794\\_9-10000.html](http://www.net-security.org/cgi-bin/news.cgi?url=http://www.idg.net/ic_274724_1794_9-10000.html)

#### IPSWITCH RATCHETS UP SECURITY IN FTP SERVER

Ipswitch Inc. released version 2.0 of its WS\_FTP server, adding several security enhancements that the company hopes will give businesses a faster, cheaper alternative to VPNs. The new iteration of WS\_FTP is essentially the first secure FTP server and gives users the added insurance of Secure Sockets Layer encryption on both the client and server sides, company officials said.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.zdnet.com/eweek/stories/general/0,11011,2643153,00.html>

## FIREWALLS AND SECURITY

"All security implementations are about striking an appropriate balance between usability and security. Increased security means decreased usability. For those who are somewhat protected by a well-configured firewall, good for you. But it may not be enough. I'll show you 3 scenarios where firewalls are not very helpful."

Link: [http://linuxtoday.com/news\\_story.php?ltsn=2000-10-22-013-04-OP-BZ-SW](http://linuxtoday.com/news_story.php?ltsn=2000-10-22-013-04-OP-BZ-SW)

## PRIVACY SOLUTIONS

The SiegeSurfer is a web-based proxy that can relay pages either through clear text or through encrypted SSL. It has a free edition which is accessible on their web site.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.siegesoft.com/>

## ONLINE BANK SECURITY BREACH HITS NORWAY

Consumer faith in online banking suffered another dent this week after four Norwegian banks admitted leaving the financial details of one million customers exposed on their internet sites for two months. The flaw was only discovered by one of the banks when a 17-year-old boy contacted a Norwegian newspaper to explain how it was possible to see the details. Services at Sparebanken Nor, Parat 24, Sparebanken More and Sparebanken Sogn og Fjordane were affected.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.uk.internet.com/Article/100713>

## SAFETY IN INTERNET SECURITY

According to International Data Corporation, the worldwide market for information security services (including consulting, integration, management, and education and training) will grow to \$16.5 billion by 2004, up from \$4.8 billion in 1998. As a growing number of companies move online, secure transactions become more important.

Link: [http://www.net-security.org/cgi-bin/news.cgi?url=http://cnfn.cnn.com/2000/10/23/redherring/herring\\_netsafety/](http://www.net-security.org/cgi-bin/news.cgi?url=http://cnfn.cnn.com/2000/10/23/redherring/herring_netsafety/)

## PUTTING PRIVACY IN PERSPECTIVE

There's a lot of sound and fury these days about privacy and the Net - about how your privacy is going to be seriously compromised soon, if it's not already; about how innovations in cell phones and global positioning satellite systems (GPSS) are going to reveal our innermost thoughts and lives; and about how our personal data is going to be sold on every street corner, to all comers.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.zdnet.com/zdnn/stories/news/0,4586,2643408,00.html>

## US NATIONAL SECURITY AGENCY BADLY CRIPPLED

Those accustomed to imagine the NSA as some guild of omniscient, malevolent hermits effortlessly deciphering all the electromagnetic noise enveloping the modern world will be bitterly disappointed to learn that its basic, functional competence is in doubt. While the Agency has been credited with miraculous achievements such as monitoring every communication made by electronic means worldwide with its famous Echelon system, there's reason to wonder if it will even exist a decade from now.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.theregister.co.uk/content/1/14170.html>

#### BROADBAND COULD BE HACKLAND

Recently, Steve Gibson, an independent software developer, received a call from the FBI. "Apparently, some hacker was getting into people's computers and posting notes on their Windows desktops," Gibson said. "The notes were telling people that their computer was insecure, and that they should go to GRC.com. So the FBI said, 'Steve, did you do this?'"

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.wired.com/news/technology/0,1282,39235,00.html>

---

#### Security issues

-----

All vulnerabilities are located at:  
<http://net-security.org/text/bugs>

---

#### HALF-LIFE DEDICATED SERVER VULNERABILITY

The vulnerability appears to exist in the changelevel rcon command and does not require a valid rcon password. The overflow appears to exist after the logging function as the following was found in the last entries of the daemon's logs.

Link: <http://www.net-security.org/text/bugs/971734269,9161,.shtml>

#### VARIOUS BUGS IN AUCTION WEAVER LITE 1.0 - 1.04

Auction Weaver LITE 1.0 through 1.04 contains several vulnerabilities that allow remote attackers to create, read, or delete arbitrary files with the privileges of the Auction Weaver process. These vulnerabilities are different than the ones described by Meliksah Ozoral and teleh0r in several Bugtraq posts during August 2000. All of the vulnerabilities are commonly found in CGI scripting programs.

Link: <http://www.net-security.org/text/bugs/971734296,24398,.shtml>

#### LOCAL ROOT COMPROMISE IN SUSE LINUX

The problem in the implementation of traceroute that we ship is a format string parsing bug in a routine that can be used to terminate a line in traceroute's output to easily embed the program in cgi scripts as used for web frontends for traceroute. Using a specially crafted sequence of characters on the commandline, it is possible to trick the traceroute program into running arbitrary code as root.

Link: <http://www.net-security.org/text/bugs/971734328,33658,.shtml>

#### MS - "WEB SERVER FOLDER TRAVERSAL" VULNERABILITY

Microsoft has released a patch that eliminates a security vulnerability in Microsoft IIS 4.0 and 5.0. The vulnerability could potentially allow a visitor

to a web site to take a wide range of destructive actions against it, including running programs on it.

Link: <http://www.net-security.org/text/bugs/971791936,23710,..shtml>

#### RED HAT - POTENTIAL SECURITY PROBLEMS IN PING FIXED

Several problems in ping are fixed:

- 1) Root privileges are dropped after acquiring a raw socket.
- 2) An 8 byte overflow of a static buffer "outpack" is prevented.
- 3) An overflow of a static buffer "buf" is prevented.

A non-exploitable root only segfault is fixed as well.

Link: <http://www.net-security.org/text/bugs/971918719,36405,..shtml>

#### SUSE LINUX - POSSIBLE REMOTE ROOT COMPROMISE

Security problems have been found in the client code of the NIS subsystem.

SuSE distributions before SuSE-6.1 came with the original ypbind program, SuSE-6.2 and later included the ypbind-mt NIS client implementation. ypbind-3.3 (the earlier version) has a format string parsing bug if it is run in debug mode, and (discovered by Olaf Kirch ) leaks file descriptors under certain circumstances which can lead to a DoS. In addition, ypbind-3.3 may suffer from buffer overflows. ypbind-mt, the software shipped with SuSE distributions starting with SuSE-6.2, suffers from a single format string parsing bug. Some of these bugs could allow remote attackers to execute arbitrary code as root.

Link: <http://www.net-security.org/text/bugs/971918769,99572,..shtml>

#### IE 5.5/OUTLOOK JAVA SECURITY VULNERABILITY

The problem is the possibility for specifying arbitrary codebase for an applet loaded from < OBJECT> tag and a jar file. Applets may read URLs from their codebase and communicate with hosts from the codebase.

Link: <http://www.net-security.org/text/bugs/971918788,31435,..shtml>

#### HYPERTERMINAL BUFFER OVERFLOW VULNERABILITY

The USSR Team has found a buffer overflow in the HyperTerminal telnet client, which is in the code that processes the Telnet URL's, that can enable an attacker to execute arbitrary code on another user's system. If a user opens an mail containing HTML and also contains a malformed Telnet URL a buffer overrun will enable the creator of the mail to cause arbitrary code to be run on the user's system.

Link: <http://www.net-security.org/text/bugs/971956137,87210,..shtml>

#### MS - "HYPERTERMINAL BUFFER OVERFLOW" PATCH

Microsoft has released a patch that eliminates a security vulnerability in the HyperTerminal application that ships with several Microsoft operating systems. This vulnerability could, under certain circumstances, allow a malicious user to execute arbitrary code on another user's system.

Link: <http://www.net-security.org/text/bugs/971956179,76463,..shtml>

#### DOS ON COMPUTERS RUNNING MICROSOFT NETMEETING

The exploit has been tested against the current version of NetMeeting 3.01 which ships with Windows 2000. It has been tested on Windows 95, NT 4 Workstation and Server SP5/6, and Windows 2000 Workstation and Server SP1. It has been tested against computers with either modem or ethernet

connections. Microsoft has released a patch for Windows 2000. At this time, there are some issues with the NT 4.0 patch installer. Microsoft is working to fix these issues, and an updated installer should be available when complete.  
Link: <http://www.net-security.org/text/bugs/971956301,13545,.shtml>

#### CALDERA LINUX - VERIFICATION BUG IN GNUPG

There is a bug in the signature verification of GNUpg, the GNU replacement for PGP. Normally, signature verification with gnupg works as expected; gnupg properly detects when digitally signed data has been tampered with. However, these checks do not work properly if there are several sections with inline signatures within a single file. In this case, GNUpg does not always detect when some of the signed portions have been modified, and incorrectly claims that all signatures are valid.

Link: <http://www.net-security.org/text/bugs/972040195,29520,.shtml>

#### DOS IN INTEL'S 'INBUSINESS EMAIL STATION'

"I found a buffer overflow in the Intel InBusiness eMail Station, which can enable an attacker to execute a denial of service attack against it."

Link: <http://www.net-security.org/text/bugs/972091882,33592,.shtml>

#### MANDRAKE & RED HAT LINUX - GNUPG UPDATE

A problem exists in all versions of GnuPG prior to and including 1.0.3. Because of this problem, GnuPG may report files which have been signed with multiple keys (one or more of which may be incorrect) to be valid even if one of the signatures is in fact valid.

Mandrake: <http://www.net-security.org/text/bugs/972138403,22492,.shtml>

Red Hat: <http://www.net-security.org/text/bugs/972138926,2985,.shtml>

#### NETMEETING DS VULNERABILITY PATCH

This patch eliminates a security vulnerability in NetMeeting, an application that ships with Microsoft Windows 2000 and is also available as a separate download for Windows NT 4.0. The vulnerability could allow a malicious user to temporarily prevent an affected machine from providing any NetMeeting services and possibly consume 100% CPU utilization during an attack.

Link: <http://net-security.org/various/software/972136197,66286,.shtml>

#### TASKPAD SCRIPTING VULNERABILITY PATCH

Eliminate a vulnerability in the TaskPads feature, which is provided as part of Microsoft Resource Kit products for Windows 95, 98 and Windows NT. The vulnerability could allow a Web site to run executables on the computer of a user who had installed one of the affected Resource Kits. The patch will check the system for the vulnerability and repair it. In addition, a measure will be introduced to prevent accidental reinstallation of the TaskPads' functionality.

Link: <http://net-security.org/various/software/972136281,83666,.shtml>

#### WEBTV VULNERABILITY PATCH (WIN 98)

This patch eliminates a security vulnerability in Microsoft WebTV for Windows. There is a Denial-of-service vulnerability in WebTV for Windows that may allow a malicious user to remotely crash either the WebTV for Windows application and/or the computer system running WebTV for Windows. Restarting the application and/or system will return the system to its normal state. Although

the WebTV for Windows application ships with Windows 98, 98SE, and Windows Me products, the application is not installed by default, and customers who have not installed it would not be at risk.

Link: <http://net-security.org/various/software/972137324,68386,.shtml>

WEFTV VULNERABILITY PATCH (WIN 2K)

Link: <http://net-security.org/various/software/972137392,43847,.shtml>

-----  
Security world  
-----

All press releases are located at:  
<http://net-security.org/text/press>

-----  
ATTACHMATE INTRODUCES E-VANTAGE HOST ACCESS SERVER V2.3 - [17.10.2000]

Attachmate Corporation announced the release of Attachmate e-Vantage Host Access Server 2.3, the latest version of Attachmate's Web-based host access management solution. Attachmate e-Vantage Host Access Server 2.3 introduces management console support on IBM's OS/390 mainframe and AS/400 host platforms, in addition to server platform support on Sun Solaris HP/UX , AIX and LINUX operating systems.

Press release:

< <http://www.net-security.org/text/press/971737900,23487,.shtml> >

-----  
ESECURITYONLINE NAMES ROBIN HUTCHINSON CEO - [18.10.2000]

Ernst & Young LLP announced today that Robin Hutchinson has been appointed CEO of eSecurityOnline, a venture of Ernst & Young LLP. eSecurityOnline provides businesses with an online security content solution to help protect against computer and Internet crime. Its offerings include vulnerability tracking, security asset management, as well as providing a portal to over one thousand security related resources.

Press release:

< <http://www.net-security.org/text/press/971737998,72858,.shtml> >

-----  
PROTECTION AGAINST NEW MICROSOFT IIS VULNERABILITY - [18.10.2000]

Network ICE's team of security experts release protection against a newly discovered exploit poised to cause significant damage to the Internet. The new vulnerability, "Multibyte Backticking," allows intruders to break into large numbers of Microsoft IIS 4.0 and 5.0 servers. Microsoft IIS servers account for roughly 20% of the websites on the Internet.

Press release:

< <http://www.net-security.org/text/press/971830658,73146,.shtml> >

---

#### SYBARI AND SOPHOS PARTNERSHIP - [18.10.2000]

Sybari Software, Inc., the premier antivirus and security specialist for groupware solutions, announced that its installed customer base will receive Sophos' award winning scan engine at no cost for the length of their existing Antigen license agreement.

Press release:

< <http://www.net-security.org/text/press/971831246,67224,.shtml> >

---

#### @STAKE PARTNERS WITH COUNTERPANE - [18.10.2000]

@stake, the world's leading Internet security consulting firm, announced an alliance with the premier Managed Security Monitoring services firm, Counterpane Internet Security, Inc. Working together, @stake and Counterpane will offer a comprehensive set of Internet security consulting and response services integrated with world-class 24 X 7 managed services.

Press release:

< <http://www.net-security.org/text/press/971881026,40424,.shtml> >

---

#### COMPUTER ASSOCIATES AND SYBARI SOFTWARE ALLIANCE - [19.10.2000]

Computer Associates International, Inc, the world's leading eBusiness solutions provider, and Sybari Software, Inc., the premier antivirus and security specialist for groupware solutions, announced an alliance designed to protect the most complex messaging infrastructures from malicious virus attacks.

Press release:

< <http://www.net-security.org/text/press/971919142,42607,.shtml> >

---

#### SECURELY MANAGING E-BUSINESS APPLICATIONS - [19.10.2000]

AXENT Technologies, Inc., one of the world's leading e-security solutions providers for e-business, who recently entered into a definitive agreement with Symantec Corporation to be acquired, and ActivCard, Inc., a leader in digital identity and electronic certification technology, announced plans to expand their long-term relationship to provide customers with flexible and versatile authentication through the use of smart card technology.

Press release:

< <http://www.net-security.org/text/press/971973401,88722,.shtml> >

---

CUSTOMIZABLE NETWORK-BASED FIREWALL SERVICE - [19.10.2000]

Businesses with broadband DSL connections can now enjoy customizable protection against intrusion and hacker attacks at a fraction of the cost of conventional, CPE-based firewalls, thanks to Firewall Flex(sm), a customizable, network-based security product from Zyan Communications.

Press release:

< <http://www.net-security.org/text/press/971973458,71081,.shtml> >

-----

HYPERTERMINAL PRIVATE EDITION 6.1 PLUGS VULNERABILITY - [20.10.2000]

Hilgraeve Inc., a long-time leader in PC data communications software, announced HyperTerminal Private Edition 6.1, as an upgrade to its HyperTerminal communications program, which Microsoft includes with every copy of Windows. This new release corrects a potentially serious security issue that affects versions of HyperTerminal included with Microsoft Windows.

Press release:

< <http://www.net-security.org/text/press/972003786,31146,.shtml> >

-----

ITALIAN COMPANY CRYPTONET PARTNERS WITH RAINBOW - [21.10.2000]

Rainbow TechnologiesTM Inc., a leading provider of high-performance security solutions for the Internet and eCommerce, and CryptoNet, an Italian company focused entirely on information security, announced a partnership agreement that permits CryptoNet to distribute Rainbow's CryptoSwift eCommerce accelerator products and iKey workstation security solutions in Italy. The agreement represents the next step in Rainbow's aggressive strategy for international distribution of products and services that provide security solutions for the Internet and international eCommerce.

Press release:

< <http://www.net-security.org/text/press/972092122,42214,.shtml> >

-----

Featured articles

-----

All articles are located at:

<http://www.net-security.org/text/articles>

Articles can be contributed to [staff@net-security.org](mailto:staff@net-security.org)

-----

TWO NEW ADDITIONS TO THE ARTICLES SECTION

The first addition is dedicated to Old School text files, that have their roots in the BBS era. This section was built in association with Textfiles.com in order to let a larger audience experience the beginnings of the "hacking" scene and the related events and thoughts.

The Old School section can be found here:

< <http://www.net-security.org/text/articles/index-oldschool.shtml> >

The second addition is made in cooperation with RADCOM, a member of the RAD Group, a leading network test and quality monitoring equipment manufacturer focused on test solutions for LANs, WANs, ATM, cellular converged networks and convergence technologies. In this section you can read documents which contain useful technical information concerning the communications industry in general and the use of RADCOM's protocol analyzers in various testing situations.

The RADCOM section can be found here:

< <http://www.net-security.org/text/articles/index-radcom.shtml> >

-----  
Following is the complete list of available articles in these two added sections.

-----  
COMPLETE LIST OF AVAILABLE PAPERS IN THE OLD SCHOOL SECTION

AT&T has declared malicious WAR

< <http://www.net-security.org/text/articles/oldschool/attrebel.shtml> >

Fun with Automatic Tellers

< <http://www.net-security.org/text/articles/oldschool/tellers.shtml> >

Hacking Calling Cards

< <http://www.net-security.org/text/articles/oldschool/callingcards.shtml> >

Free CompuServe Passwords

< <http://www.net-security.org/text/articles/oldschool/compus.shtml> >

Tapping Computer Data Is Easy

< <http://www.net-security.org/text/articles/oldschool/datatap.shtml> >

CIRR Database

< <http://www.net-security.org/text/articles/oldschool/database.shtml> >

Acronyms 01

< <http://www.net-security.org/text/articles/oldschool/acro1.shtml> >

Acronyms 02

< <http://www.net-security.org/text/articles/oldschool/acro2.shtml> >

List of Computer Hackers News Articles

< <http://www.net-security.org/text/articles/oldschool/articls.shtml> >

Hackers Penetrate DOD Computer Systems

< [http://www.net-security.org/text/articles/oldschool/com\\_sec91.shtml](http://www.net-security.org/text/articles/oldschool/com_sec91.shtml) >

For Your Protection

< <http://www.net-security.org/text/articles/oldschool/crackdown.shtml> >

The CyberPunk Movement

< <http://www.net-security.org/text/articles/oldschool/cyber.shtml> >

Dial Back isn't always secure

< <http://www.net-security.org/text/articles/oldschool/dialback.shtml> >

The FBI fights computer crime...

< <http://www.net-security.org/text/articles/oldschool/fbiafta.shtml> >

Diary of a Hacker

< <http://www.net-security.org/text/articles/oldschool/hacker1.shtml> >

The Hacker's Song

< <http://www.net-security.org/text/articles/oldschool/hacksong.shtml> >

The History of Hacking and Phreaking

< <http://www.net-security.org/text/articles/oldschool/his-hp.shtml> >

Pumpcon

< <http://www.net-security.org/text/articles/oldschool/pumpcon.shtml> >

The Phrack E911 Affair

< <http://www.net-security.org/text/articles/oldschool/2600dox.shtml> >

Planning Ahead

< <http://www.net-security.org/text/articles/oldschool/avoidcap.shtml> >

Data General

< <http://www.net-security.org/text/articles/oldschool/datagen.shtml> >

Bell Trashing

< [http://www.net-security.org/text/articles/oldschool/garbake\\_phk.shtml](http://www.net-security.org/text/articles/oldschool/garbake_phk.shtml) >

Hacking Voice Mail Systems

< <http://www.net-security.org/text/articles/oldschool/voicemail.shtml> >

HoHoCon 1993

< <http://www.net-security.org/text/articles/oldschool/hohocon.shtml> >

[ The History of MOD ] - book one

< <http://www.net-security.org/text/articles/oldschool/mod1.shtml> >

[ The History of MOD ] - book two

< <http://www.net-security.org/text/articles/oldschool/mod2.shtml> >

[ The History of MOD ] - book three

< <http://www.net-security.org/text/articles/oldschool/mod3.shtml> >

[ The History of MOD ] - book four

< <http://www.net-security.org/text/articles/oldschool/mod4.shtml> >

[ The History of MOD ] - book five

< <http://www.net-security.org/text/articles/oldschool/mod5.shtml> >

-----

## COMPLETE LIST OF AVAILABLE DOCUMENTS IN THE RADCOM SECTION

How to Analyze LAN Traffic Over ATM

< <http://www.net-security.org/text/articles/dl/radcom/an5294.pdf> >

How to Test ATM SONET/SDH Lines

< <http://www.net-security.org/text/articles/dl/radcom/an4994.pdf> >

How to Verify Data Integrity Through an ATM Network

< <http://www.net-security.org/text/articles/dl/radcom/an0495.pdf> >

How to Integrate FORE Systems Equipment with SPANS Signalling

< <http://www.net-security.org/text/articles/dl/radcom/an0695.pdf> >

Effective PPP Testing

< <http://www.net-security.org/text/articles/dl/radcom/ppp.pdf> >

ISDN Testing

< <http://www.net-security.org/text/articles/dl/radcom/wl42.pdf> >

Internet Protocol Analyzer

< <http://www.net-security.org/text/articles/dl/radcom/wl46.pdf> >

IP Blaster

< <http://www.net-security.org/text/articles/dl/radcom/ipblaste.pdf> >

ISDN Simulation

< <http://www.net-security.org/text/articles/dl/radcom/isdnsim.pdf> >

Live Protocol Analysis

< <http://www.net-security.org/text/articles/dl/radcom/liveprot.pdf> >

RC-155-C Script Language

< <http://www.net-security.org/text/articles/dl/radcom/script.pdf> >

-----  
  
Featured books  
-----

The HNS bookstore is located at:

<http://net-security.org/various/bookstore>

Suggestions for books to be included into our bookstore  
can be sent to [staff@net-security.org](mailto:staff@net-security.org)

-----  
  
HACKING EXPOSED - SECOND EDITION

The book describes the security characteristics of several computer-industry pillars, including Windows NT, Unix, Novell NetWare, and certain firewalls. It also explains what sorts of attacks against these systems are feasible, which

are popular, and what tools exist to make them easier. The authors walk the reader through numerous attacks, explaining exactly what attackers want, how they defeat the relevant security features, and what they do once they've achieved their goal. In what might be called after-action reports, countermeasures that can help steer bad buys toward less-well-defended prey are explained. Topics covered: The state of the art in breaking into computers and networks, as viewed from the vantage point of the attacker and the defender. There's information on surveying a system remotely, identifying weak points, and exploiting weaknesses in specific operating systems (Windows NT, Unix, and Novell NetWare, mostly). Coverage also includes war dialers, circumventing firewalls, denial-of-service attacks, and remote-control software. There's a cool appendix on the security characteristics of Windows 2000.

Book:

< <http://www.amazon.com/exec/obidos/ASIN/0072127481/netsecurity> >

---

#### PROFESSIONAL JAVA 2 ENTERPRISE EDITION WITH BEA WEBLOGIC SERVER

Business objects are basically encapsulated business processes that deal with some input data and mediate the appropriate business response. Professional J2EE Programming with BEA Web Logic Server shows how suited to the creation of business objects and the n-tier applications centered on them Java is. Key areas covered include real world techniques for application development, explanation of how to create business logic components from Enterprise Java Beans, database handling with JDBC, JNDI and directory services, Java messaging services and interfacing applications to CORBA/DCOM systems and XML.

Book:

< <http://www.amazon.com/exec/obidos/ASIN/1861002998/netsecurity> >

---

#### LINUX ASSEMBLY LANGUAGE PROGRAMMING

Explains all the key features of c86 assembly language in the context of Linux operating system and the C language. Uses a step-by-step, one-concept-at-a-time coverage to help the user master essentials skills. CD-ROM includes the Open Source assembler NASM, edinas, and sample device drivers from the text.

Book:

< <http://www.amazon.com/exec/obidos/ASIN/0130879401/netsecurity> >

---

#### TOMES OF DELPHI: ALGORITHMS AND DATA STRUCTURES

Tomes of Delphi: Algorithms and Data Structures is a highly sophisticated title targeted for advanced developers. Author Julian Bucknall works for one of Inprise's leading and oldest third-party library and tool companies, TurboPower, where he is in charge of technical development. This is the only book on the market that will provide Delphi developers with a comprehensive and current overview of using algorithms and data structures from a practical, not a theoretical, textbook perspective. The book will include a wealth of code

examples appropriate for practicing developers. Bucknall's title will provide comprehensive coverage of such topics as binary trees, data compression, and other advanced topics not treated in any competing titles. The CD includes the author's highly successful freeware library EZDSL along with the code from the book.

Book:

< <http://www.amazon.com/exec/obidos/ASIN/1556227361/netsecurity> >

---

#### THE JAVA DEVELOPERS ALMANAC 2000 (THE JAVA SERIES)

This book provides a truly valuable reference to nearly all the classes and APIs in standard Java. This "white pages" for Java puts all classes and APIs at your fingertips, along with short samples that illustrate essential programming tasks. It's a compliment to say that this title resembles a telephone book. With over 1,000 pages (and printed on similar paper stock), The Java Developers Almanac, like a phone book, is organized alphabetically. Early sections look at Java 2 classes by package, such as graphics (including Java 2D), file I/O, network programming, and AWT and Swing. Early sections include several hundred short code excerpts, which provide key programming solutions. The heart of this text is an A-to-Z compendium of over 2,100 Java classes, and a whopping 24,000 methods and properties.

Book:

< <http://www.amazon.com/exec/obidos/ASIN/0201432994/netsecurity> >

---

#### Security Software

---

All programs are located at:

<http://net-security.org/various/software>

---

#### VLAD THE SCANNER V0.7.4

VLAD the Scanner is an open-source security scanner that checks for the SANS Top Ten security vulnerabilities commonly found to be the source of a system compromise. It has been tested on Linux, OpenBSD, and FreeBSD.

Link:

< <http://net-security.org/various/software/971974205,30976,.shtml> >

---

#### SPAMMOTEL V.1.2.1

A unique web-based anti-spam program that gives you complete control of your e-mail address, without the use of filters. SpamMotel gives you a special 'disposable' e-mail address each time you use it, and lets you

attach a reminder memo to it. Any e-mail sent to that special address is forwarded to your regular e-mail account, along with your memo, which appears at the top of the incoming e-mail message. You'll know exactly when and where the spammer got your e-mail address. Use the handy online Log Page to control these special addresses and block any sender. This free program works with your existing e-mail account. A download-able interface makes access easy, and requires no installation on your computer. Also useful in organizing your e-mail folders more effectively.

Link:

< <http://net-security.org/various/software/971647417,19204,.shtml> >

---

#### SAFEGUARD PRIVATECRYPT

SafeGuard PrivateCrypt an easy to use encryption application supporting the new AES algorithm. Thus it is one of the fastest and most secure encryption tools worldwide. And one of the easiest - without authorization of the recipient, without exchange of keys.

Link:

< <http://net-security.org/various/software/971974861,31291,.shtml> >

---

#### BASTILLE LINUX V.1.1.1

Bastille Linux aims to be the most comprehensive, flexible, and educational Security Hardening Program for Red Hat Linux 6.0/6.1. Virtually every task it performs is optional, providing immense flexibility. It educates the installing admin regarding the topic at hand before asking any question. The interactive nature allows the program to be more thorough when securing, while the educational component produces an admin who is less likely to compromise the increased security.

Link:

< <http://net-security.org/various/software/971974996,81622,.shtml> >

---

#### Defaced archives

---

[16.10.2000] - Anti-AOL

Original: <http://www.anti-aol.org/>

Defaced: <http://www.attrition.org/mirror/attrition/2000/10/16/www.anti-aol.org/>

[16.10.2000] - United States Department of Transportation

Original: <http://stratplan.dot.gov/>

Defaced: <http://www.attrition.org/mirror/attrition/2000/10/16/stratplan.dot.gov/>

[16.10.2000] - National Institutes of Health

Original: <http://intra.ninds.nih.gov/>

Defaced: <http://www.attrition.org/mirror/attrition/2000/10/16/intra.ninds.nih.gov/>

[16.10.2000] - Administrative Office of the U.S. Courts

Original: <http://www.mab.uscourts.gov/>

Defaced: <http://www.attrition.org/mirror/attrition/2000/10/16/www.mab.uscourts.gov/>

[16.10.2000] - Multistate Tax Commission

Original: <http://www.mtc.gov/>

Defaced: <http://www.attrition.org/mirror/attrition/2000/10/16/www.mtc.gov/>

[16.10.2000] - State of California

Original: <http://www.pia.ca.gov/>

Defaced: <http://www.attrition.org/mirror/attrition/2000/10/16/www.pia.ca.gov/>

[16.10.2000] - Panasonic (PL)

Original: <http://www.panasonic.com.pl/>

Defaced: <http://www.attrition.org/mirror/attrition/2000/10/16/www.panasonic.com.pl/>

[17.10.2000] - Linux Center (AR)

Original: <http://www.linuxcenter.com.ar/>

Defaced: <http://www.attrition.org/mirror/attrition/2000/10/17/www.linuxcenter.com.ar/>

[18.10.2000] - Family Serv

Original: <http://www.familyserv.org/>

Defaced: <http://www.attrition.org/mirror/attrition/2000/10/18/www.familyserv.org/>

[21.10.2000] - The Scottish Legal Life Assurance Society Ltd.

Original: <http://www.scotlegal.com/>

Defaced: <http://www.attrition.org/mirror/attrition/2000/10/21/www.scotlegal.com/>

[21.10.2000] - Gamers Network GmbH

Original: <http://www.planetfifa.de/>

Defaced: <http://www.attrition.org/mirror/attrition/2000/10/21/www.planetfifa.de/>

-----  
Questions, contributions, comments or ideas go to:

Help Net Security staff

[staff@net-security.org](mailto:staff@net-security.org)

<http://net-security.org>