

ISS to offer free security patch after being slammed for 'selling' security patches

Psssst buddy... want to buy a patch...

Yahoo and Hotmail e-mail accounts at risk by severe security vulnerability

Remotely Exploitable Cross-Site scripting in Hotmail and Yahoo

Black Ice flaw leads to tens of thousands of computers being damaged

Worm destroyed or damaged tens of thousands of personal computers worldwide Saturday morning

World largest series of raids against movie and entertainment software piracy

Raids ongoing in Europe and elsewhere with hundreds busted

Hacker Retaliator - New Security product strikes back at hackers

Returns equal fire at hackers promises Symbiot

Three more patches from Microsoft for Office XP, MSN Messenger & MS Windows

Not life or death critical but Office XP rated important

emergency response team. TCP – the Transmission Control Protocol – contains a flaw that "varies by vendor and application, but in some deployment scenarios...is rated critical," said the advisory, published by the United Kingdom's National Infrastructure Security Co-ordination Centre. Networking-hardware maker Juniper Networks has determined that its products are vulnerable. Cisco Systems, Hitachi, NEC, and others are studying the issue, according to the advisory. The vulnerability allows for what's known as a reset attack. Many network appliances and software programs rely on a continuous stream of data from a single source – called a session – and prematurely ending the session can cause a wide variety of problems for devices. Security researcher Paul Watson discovered a method that makes disrupting the data flow far easier than previously thought.

The center's advisory is based on security research that Watson plans to present at the CanSecWest 2004 conference this week and apparently had been released a day early by the NISCC, according to the conference organizer. Watson, who runs a pro hacking blog at Terrorist.net, could not be reached for comment. The issue of TCP-related reset attacks has surfaced before – discussions of the flaw on a mailing list for large-network operators dismissed the issue as old news – but they've previously been thought to require the attacker to guess the identifier of the next data packet in a session. The odds on that are about one in 4.3 billion. The NISCC advisory argues that Watson's research shows that any number in a certain window of values will work, making it much more likely that such an attack could succeed. The effect of resetting a connection varies depending on the application and how resistant the network software is to disruption, the advisory said. Under certain circumstances, an attack could significantly disrupt the network used by the basic devices of the Internet, known as routers, to map the most efficient data path from one server to another. Known as the Border Gateway Protocol, or BGP, the method of passing routing information relies on long-lived sessions, and disturbing those connections could cause "medium-term unavailability," the advisory said....continued....

HeadlineViewer

Amphetadesk

Radio Userland

Live Online Chat Rooms
(Click here to Enter Chat)

Users Now in Chat Rooms

- MainLobby (1)
👤 shmss
- WaterCooler (0)
- ServerRoom (0)
- TheCubicle (0)
- BoardRoom (0)
- HamstersPlace (0)
- AfterHoursBar (0)



Click here to read the full story at
CNET's News.com

**Here are some more stories
reporting on this new vulnerability**

- **Serious New Internet Security Flaw** - Netlawblog (Weblog)
- **Security Vulnerability Threatens Internet Protocol** - Network Magazine
- **Multiple Vendor TCP Sequence Number Approximation Vulnerability** - Symantec - Security Update on Threats
- **Cisco Security Advisory: TCP Vulnerabilities in Multiple IOS-Based Cisco Products** - SecurityFocus.com
- **Security Vulnerability Threatens Internet** - Information Week
- **TechBrief: Flaw found in security of Internet** - International Herald Tribune
- **Internet Jeopardized by Serious Security Flaw** - Geek News Central (Weblog)
- **Widespread Net Security Flaw Found** - PC World
- **Cisco Security Advisory: TCP Vulnerabilities in Multiple Non-IOS Cisco Products** - SecurityFocus.com
- **Multiple Vendor TCP Stack Implementations Let Remote Users Deny Service** - Security Tracker
- **Underlying Internet Technology Vulnerable to Hackers** - RedNova
- **Protocol Of Internet Backbone Vulnerable To Hacks** - TheIowaChannel.com, Iowa

Latest Security News

From **News Now >**

SCO Sweats as BayStar

Netsky-V worm can infect computers without e-mail attachment being clicked

No need to double-click to be infected by Netsky -V
04-15-2004 10:25:12 AM CST - from the folks at Sophos

Comment about this story **Read** Comments posted about this story...

Latest S

To

Threatens To Pull Funds
NewsFactor

Training will turn receptionists
into security gurus
Silicon.com

GVI Security Solutions, Inc.
Wins Major U.S. Port Security
Contract
TMCnet.com Registration site:

Adding multicast to IPSec
Techworld

Web security standard is go,
go, go!
Techworld

Mandrake MDKSA-2004:032:
libneon
SecurityFocus.com

Mandrake MDKSA-2004:033:
xine-ui
SecurityFocus.com

Brits are crap at password
security
The Register

Apple Breaks into Storage
Area Networks
NewsFactor

Microsoft Picks Up Hackers'
Gauntlet
NewsFactor

Security Switch Assures
Significant Savings
SourceWire (Press Release)

BorderWare Announces
MXtreme Mail Firewall
Version 4.0
SourceWire (Press Release)

MXtreme, Industry's First Mail
Firewall to Deliver Zero
Downtime, Zero Latency, Zero
Message Loss
SourceWire (Press Release)

ArX libneon Client Code
Format String Vulnerabilities
Secunia

No need to double-click to be infected by Netsky-V the new Netsky-V worm (W32/Netsky-V) spreads without using email attachments to infect. Other widespread versions of the Netsky worm have infected users by tempting them to double-click on an email attachment, but Netsky-V exploits security loopholes in Microsoft's software that mean users can be hit just by reading an email. Emails containing the exploit, which can use subject lines such as 'Converting message. Please wait...' and 'Please wait while loading failed message...', attempt to download a copy of the worm from another user's computer. "Home users are especially vulnerable to this kind of attack as their computers are often not properly protected with a personal firewall or the latest anti-virus updates," said Graham Cluley, senior technology consultant for Sophos. "Personal computer users should consider checking out Microsoft's security update website, which can scan home PCs for security vulnerabilities and suggest which critical patches need to be installed."

Sophos recommends that computer users monitor announcements from operating system, application and web server software vendors for details of new vulnerabilities found in their code. Many viruses have exploited loopholes in commonly used web browsers and email software to increase their chances of spreading effectively. Loopholes are found in products on a weekly basis, some significant, some trivial. "IT managers should keep abreast of these loopholes and apply patches where appropriate before new viruses come along to exploit them," continued Cluley.

Home users of Microsoft Windows can visit :
<http://windowsupdate.microsoft.com>
to have their systems scanned for Microsoft security vulnerabilities.

- [Click here to see what Panda has to say about Netsky.V](#)
- [Click here to see what Sophos has to say about Netsky-V](#)
- [Click here to see what TrendMicro has to say about NETSKY.V](#)
- [Click here to see what McAfee has to say about Netsky.v](#)
- [Click here to see what Symantec has to say about Netsky.V](#)
- [Click here to see what Computer Associates has to say...](#)
- [Click here to see what F-Secure has to say about NetSky.V](#)

Isn't that just the way things go... the dumb users are finally learning to not click on every attachment that falls into their mail box and now along comes a worm that doesn't require any clicks... ouch... now we have to depend on the dumb users to keep their anti-virus software and their operating systems patched and updated... argh...

Microsoft issues new patches to secure against at least 20 Windows vulnerabilities

Windows operating system vulnerable to new worms or viruses
04-13-2004 5:52:45 PM CST - by Robert Lemos for CNET's News.com

S

Hc
Fc

Ple:

Security
15 News

Core Inter
Vulnerable
schshd, F
08:48:54

Microsoft
HTML For
Reply)
protex, Th
19:13:45

Is there a
Patching?
digitalpimj
19:03:28

How soph
phishing s
digitalpimj
18:48:25

Bagle.J ar
(2 Replies
digitalpimj
18:36:52

TCP Rese
Replies)
AplusWet
2004 17:5

best snort
AhClem, 1
09:53:41

Best Spor
Replies)
infosys, T
22:38:40

"Netsky" r
(7 Replies
AplusWet
2004 20:5

Power use

Kanguru Solutions Teams with Panasonic to Provide Unique Storage Solution for Video Security Systems
TMCnet.com

Exchange Server SMTP AUTH Attacks
Windows & .Net Magazine Network

Hacker Profile: Jericho
Hacktivism0

Passwords for Chocolate - broadbandreports.com

Serv-U FTP Server LIST Command Denial of Service Vulnerability
Secunia

BorderWare Announces MXtreme Mail Firewall Version 4.0; New Features, Functionality Set The Benchmark For...
TMCnet.com

BorderWare Technologies Inc.: MXtreme Now Industry's First Mail Firewall To Deliver Zero Downtime, Zero...
TMCnet.com

Frame Grabber suits security and monitoring applications. Industrial News Room (Press Release)

WS-Security receives official blessing from OASIS
InfoWorld

SCT Campus Pipeline Email Attachment Script Injection Vulnerability
SecurityFocus.com

Anti-virus protection: too little, too late?
Network Times

Hardware security reduces costs without compromising network performance
Network Times

New hacking tool: chocolate

Comment about this story **Read** Comments posted about this story...

Microsoft released on Tuesday fixes that cover at least 20 Windows flaws, several of which could make versions of the operating system vulnerable to new worms or viruses. At least six of the flaws could make the OS susceptible to programs similar to the MSBlast worm and its variants, which have infected more than 8 million computers since last August. Another flaw affects a common file used by Internet Explorer, Outlook and Outlook Express and opens the way for the type of virus that executes when PC users click a specially crafted Web link. The software giant released four patches to cover the 20 security issues, as part of its monthly update schedule. Microsoft wouldn't comment on the level of risk the flaws present, instead maintaining that companies that apply the fixes won't be in danger.

"If you are running a personal firewall, you are at reduced risk from a lot of these vulnerabilities," said Stephen Toulouse, security program manager for the Microsoft Security Response Center. "But we are absolutely taking this seriously." The largest patch, MS04-011, fixes at least 14 security flaws. A security hole in the Help and Support Center affects both Windows 2003 and Windows XP. Another flaw in the Windows Meta File image format could allow an attacker to create a digital picture file that could take control of a Windows NT, 2000 or XP computer. At least six of the 14 flaws could result in a remote user taking control of a Windows computer....continued....

[Click here to read the full story at CNET's News.com](#)

Click below to go directly to the appropriate Security Bulletin from Microsoft

- **MS04-014** Vulnerability in the Microsoft Jet Database Engine Could Allow Code Execution (837001)
- **MS04-013** Cumulative Security Update for Outlook Express (837009)
- **MS04-012** Cumulative Update for Microsoft RPC/DCOM (828741)
- **MS04-011** Security Update for Microsoft Windows (835732):

ISS to offer free security patch after being slammed for 'selling' security patches

Psssst buddy... want to buy a patch...
03-30-2004 09:12:16 AM CST - Munir Kotadia for ZDNet UK

Comment about this story **Read** Comments posted about this story...

ISS's security products were last week attacked by the Witty worm but the company is refusing to provide patches to customers who do not have a valid maintenance contract. Security vendor ISS has been slammed for only providing security patches to customers who have purchased a maintenance agreement from the company. Last week, this left about 12,000 computers vulnerable to the Witty

Replies)
protex, Tu
19:30:37

Security+
pipesbi, M
13:07:30

Hardening
disable wf
windows (protex, Su
19:07:46

So guys w
CISSP, C
CeeGee, I
21:12:54

Exploits A
Vulns **P.
Replies)
AplusWeb
2004 19:3

Proxy Typ
Sparky, F
12:45:03

Recent :



Bagle, N virus au
Virii wars to
hardest ?

New Biz ICQ inst users
Jokeworld.bi
personal infc

Suicide Group V Hacked
Jihad ac
groups o
site...nat

ZoneAla massive

ZDNet

Linux Kernel setsockopt
MCAST_MSFILTER Integer
Overflow Vulnerability
Secunia

Chocolate melts IT security
electricnews.net

Alerts Warn Of Massive New
Worm
Designtechnica

Phishers using smarter hooks
vnunet.com

NCSP puts security onus on
vendors
Geek.com

Passwords revealed by sweet
deal
NeoWin.net

Robert M. McNamara, Jr.
Joins OmniTrust Security
Systems, Inc. Advisory Board;
Former CIA General...
TMCnet.com

Most People Will Trade Their
Passwords For Candybars
Hacktivism

Giving Up Passwords For
Chocolate
Slashdot

One third of email now spam
The Register

Fastream NETFile FTP/Web
Server Invalid Credentials
Denial of Service
Secunia

worm, which has proved one of the most destructive worms to be released for a number of years. The Witty worm started to spread less than two days after a flaw in Internet Security Systems (ISS) RealSecure and BlackIce products was disclosed. The worm is unusual in that it is one of the first worms in recent years to have a physically destructive payload – it was designed to regularly write small amounts of data to random places on an infected machine's hard drive, which causes loss of data and eventually crashes the computer.



The ISS Patch Nazi Kitchen... "no patch for you... well maybe just one... "

Johan Beckers, director of technology solutions at ISS EMEA, told ZDNet UK that all of ISS's "legal" customers could have updated their systems to avoid Witty but he admitted that the 12,000 systems affected by Witty were most likely to be companies that had let their maintenance agreements expire: "All our products had an update available to prevent the attack from happening -- this was available to all customers that had paid their maintenance and were legal customers. If you don't pay maintenance, you are not allowed to use the products any

Zonelab extc
subscription

Microso Explore to upgra

If you can't u
execution fe
immediately

New Ba appears mail

It is picking t
an epidemic

Belgium female v Gigabyt

Could face 3
fine

Window leak 'noi

Now the job
the person v

Sophos protecti big gap

Virus or troje
boundary ca

Microso patches vulnerat

Virtual PC fc
Naming Sen
vulnerable

more," he said.

ZDNet UK suggested to Beckers that this could be interpreted as irresponsible behaviour because the company's customers that had let their contracts expire were originally sold flawed products. At this point, he said that the company would investigate the matter further and clarify the situation. At the time of writing, ISS had not provided a subsequent response. Unsurprisingly, ISS customers and security experts have criticised the company for not providing protection against known vulnerabilities to all customers, regardless of their maintenance contracts.... continued....

[Click here to read the full story at ZDNet UK](#)

UPDATE APRIL 6 : ISS has said that all customers, regardless of their maintenance contracts, will be able to download a patch to protect themselves from the Witty worm - for now. Internet Security Systems (ISS) has lifted the restrictions it had placed on out-of-contract customers who were initially denied the ability to download a security patch in order to protect themselves from the destructive Witty worm, which took advantage of a flaw in ISS' RealSecure and BlackIce products. However, ISS customers without a maintenance agreement should update their products immediately, because according to a statement from the company's press office, the free patch will only be available until 15 May, 2004.

Uh... what can I say... after initially trying the cash grab for their patches, the folks at ISS showed some common sense and have relented to let their 'non-subscribers' have the patch to secure their product. Better hurry though... their kind offer ends on May 15th..

Most Read Security News Stories From NewsNow

VeriSign Issues Alert on Massive New Worm Targetting SSL Servers
DevChannel

007 laptops: portable PCs with extra security
ZDNET US Notebook Reviews

Office Workers Willing To Leak Passwords for Chocolate
Internet Week

Office Workers Leak Passwords for Chocolate
Banktech

The more basic the better, security report recommends

Government Computer News

'Phishing' scams luring more
users
CNET

Universities, research centers
retrench after hacks
The Globe And Mail

Security strategy complete
Federal Computer Week

EarthLink aims to block
'phishing' scams
CNET

Next on FTC's Hit List:
Spyware
NewsFactor

Solaris 10 Security
SecurityFocus.com

Signs of new worm on the
way
SC Magazine

Press Release
Electronic Frontier Foundation

Microsoft picks up hackers'
gauntlet
vnunet.com

Modwest Hosts SANS
Security Seminar
TheWhir

iproute denial of service
Debian Security
Announcements

The Password Is: Chocolate
Information Week

PostNuke NS-Polls Input
Validation Hole in 'pn_uid'
Permits SQL Injection
Security Tracker

Phorum SQL Injection
Vulnerability
Secunia

New Phatbot worm may be on
the loose
ZDNet

Hackers introduce colourful
new players to Indonesia's
elections
TerraNet

phpBugTracker Multiple
Vulnerabilities
Secunia

Rumor of Internet 'Super'
Exploit
ExtremeTech

Internet crimes and security
Computer Crime Research
Center

Sophos Enters Small
Business Security Market
TechWeb

Ray-sing the security bar
USA Today

Active Network Monitor 1.31 -
a tool for the day-to-day
monitoring of computers on...
Help Net Security

Phatbot Worm May Be
Attacking SQL Server Ports
TechWeb

SECPay and ai Corp form
strategic alliance for online
payment security
M2 (Press Release)

Phorum Input Validation Hole
in 'phorum_uriauth' Lets
Remote Users Execute SQL
Commands
Security Tracker

Is Security Software Greek to
You?
WebReference.com

**Security News from
elsewhere on the Net...**

Santa Clara ready for
wireless

Climbing firewalls

Company to license device-
security tools

Data security: expect the
unexpected

Office workers sick of
passwords

Wireless security tops U.S.-
China trade talks

The Trojan that wasn't

EarthLink uncovers rampant
spyware and trojans

How cooperation can beat
viruses

Teen saves Gates from
hackers, gets nothing

Pushing to wiretap 'push to
talk'

U.K. spammers elude
shutdown

Hackers hit supercomputing
giants

Get the right virus protection

Watch out: There's an ID thief
about

Bad plumbers and leaking
software

Hackers crack research
institutions

Cisco releases WLAN
security protocol

Users warned over new
Netsky threat

Computer crime classification