

SecurityFocus Microsoft Newsletter #75

Source: <http://www.derkeiler.com/Mailing-Lists/securityfocus/focus-ms/2002-02/0203.html>

From: Marc Fossi (mfossi@securityfocus.com)

Date: 02/25/02

Date: Mon, 25 Feb 2002 13:45:32 -0700 (MST)
From: Marc Fossi <mfossi@securityfocus.com>
To: Focus-MS <focus-ms@securityfocus.com>

SecurityFocus Microsoft Newsletter #75

This Issue is Sponsored by: Stonesoft Inc.

Stonesoft is among the most trusted names in high availability software designed to reinforce all market-leading firewalls. Today, StoneBeat® FullCluster(TM) is the only high availability solution that enhances Microsoft's Internet Security & Acceleration Server with fault-tolerance and transparent failover, network-level scalability, and true dynamic load balancing.

To learn more, visit our Web site at:

<http://www.stonesoft.com/products/main/isa>

or Call 866-869-4075 or contact us at ISAServer@stonesoft.com.

I. FRONT AND CENTER

1. Future Defenses: Technologies to Stop the Unknown Attack
2. The Microsoft UPnP (Universal Plug and Play) Vulnerability
3. Network Intrusion Detection Signatures, Part Three
4. The Science of Happy Accidents
5. Secrecy Bill Doesn't Go Far Enough

II. MICROSOFT VULNERABILITY SUMMARY

1. Phusion Webserver Directory Traversal Vulnerability
2. Phusion Webserver Long URL Denial Of Service Vulnerability
3. Phusion Webserver Long URL Buffer Overflow Vulnerability
4. FastTrack P2P Technology Message Service Identity Spoofing...
5. restricting permissions for services in Win2K (Thread)
6. FastTrack P2P Technology Message Service Denial Of Service...
7. Dino's Webserver Denial of Service Vulnerability
8. GNUJSP File Disclosure Vulnerability
9. Multiple Vendor HTTP CONNECT TCP Tunnel Vulnerability

III. MICROSOFT FOCUS LIST SUMMARY

1. Security tool (Thread)
2. Unsigned Windows 2000 Patches (Thread)
3. Exchange Security (Thread)
4. Cached Domain Password on Notebook, secure? (Thread)
5. restricting permissions for services in Win2K (Thread)
6. Restrict Access to drives (Thread)
7. quick question... (Thread)
8. reading data from RAM (Thread)
9. SecurityFocus Microsoft Newsletter #74 (Thread)
10. Extra Encryption On SAM file other than md4 and syskey (Thread)
11. FW: reading data from RAM (Thread)
12. SQL SA password (Thread)
13. How to turn on the Macro prompt on MS Of (Thread)
14. Windows CE (Thread)
15. RFC (Thread)

IV. NEW PRODUCTS FOR MICROSOFT PLATFORMS

1. SafeWord
2. SoftClan e-cryptor
3. Norton Internet Security 2002
4. WebAgain

V. NEW TOOLS FOR MICROSOFT PLATFORMS

1. File::Scan v0.05
2. MIMEDefang v2.5
3. nmbscan v1.2.1

VI. SPONSORSHIP INFORMATION

I. FRONT AND CENTER

1. Future Defenses: Technologies to Stop the Unknown Attack by Nicholas Weaver

Current anti-virus software serves as a reasonably good defense against the current classes of virus, worms, and script kiddies. Unfortunately current AV solutions may not be sufficient to stop a speed-optimized active worm based on a heretofore undiscovered vulnerability. This article examines three technologies that offer significant levels of protection against unknown attacks: software fault isolation, intrusion detection through program analysis, and fine-grained mandated access controls.

<http://online.securityfocus.com/infocus/1547>

2. The Microsoft UPnP (Universal Plug and Play) Vulnerability by Paul Schmehl

On December 20, 2001, eEye Digital Security, the security firm that gave the Code Red worm its name, announced the discovery of "major security vulnerabilities"[1] in Microsoft's flagship operating system, Windows XP. Specifically, the vulnerabilities were discovered in Microsoft's Universal Plug and Play feature, which ships by default with XP. On that same day Microsoft released a patch [2] that resolved the issue; however,

it was a dismal ending to a year that saw security flaws in Microsoft products announced in the press on a weekly basis [3] and exploited in hundreds of thousands of computers worldwide.

<http://online.securityfocus.com/infocus/1548>

3. Network Intrusion Detection Signatures, Part 3 by Karen Kent Frederick

This is the third in a series of articles on understanding and developing signatures for network intrusion detection systems. In Part One and Part Two, we examined the use of IP protocol header values, particularly TCP, UDP and ICMP, in network intrusion detection signatures. In this article, we will continue our discussion of signatures by studying the area of protocol analysis, focusing on the examination of values within TCP and UDP payloads. Network intrusion detection using protocol analysis-based signatures is very effective in detecting both known and unknown attacks involving protocols such as DNS, FTP, HTTP and SMTP.

<http://online.securityfocus.com/infocus/1544>

4. The Science of Happy Accidents by Jon Lasser

The Sardonix project aims to make open source software more rigorously secure. To succeed, it will have to recreate the spontaneous magic of community that gives the movement its spark.

<http://online.securityfocus.com/columnists/62>

5. Secrecy Bill Doesn't Go Far Enough By Mark Rasch

Why is personal secrecy such a talisman, but corporate secrecy an anathema to privacy advocates?

<http://online.securityfocus.com/columnists/61>

II. BUGTRAQ SUMMARY

1. Phusion Webserver Directory Traversal Vulnerability

BugTraq ID: 4117

Remote: Yes

Date Published: Feb 16 2002 12:00A

Relevant URL:

<http://www.securityfocus.com/bid/4117>

Summary:

Phusion Webserver is a commercial HTTP server that runs on Microsoft Windows 9x/NT/2000 operating systems.

Phusion Webserver is prone to directory traversal attacks. It is possible to break out of wwwroot using triple-dot-slash (...) sequences containing HTTP-encoded variations of "/" and "\". As a result, a malicious web user may browse web-readable files on the host running the vulnerable software. This issue is due to insufficient validation of externally-supplied input.

This vulnerability may potentially result in the disclosure of sensitive information contained in web-readable files on the host. Information gathered in this manner may be used in further "intelligent" attacks against the host.

It should be noted that web servers normally run with SYSTEM privileges on Microsoft Windows operating systems.

2. Phusion Webserver Long URL Denial Of Service Vulnerability

BugTraq ID: 4118

Remote: Yes

Date Published: Feb 16 2002 12:00A

Relevant URL:

<http://www.securityfocus.com/bid/4118>

Summary:

Phusion Webserver is a commercial HTTP server that runs on Microsoft Windows 9x/NT/2000 operating systems.

Due to insufficient bounds checking, it is possible for a remote attacker to deny service to legitimate users of the service by submitting an excessively long web request (approximately 3000+ bytes).

The service must be restarted to regain normal functionality.

It should be noted that this issue is due to a remotely exploitable buffer overflow condition.

3. Phusion Webserver Long URL Buffer Overflow Vulnerability

BugTraq ID: 4119

Remote: Yes

Date Published: Feb 16 2002 12:00A

Relevant URL:

<http://www.securityfocus.com/bid/4119>

Summary:

Phusion Webserver is a commercial HTTP server that runs on Microsoft Windows 9x/NT/2000 operating systems.

Phusion Webserver does not perform sufficient bounds checking of externally supplied data in the HTTP GET requests. As a result, it is possible for a remote attacker to submit an excessively long web request which may cause stack variables, including the return address, to be overwritten. Arbitrary code execution is possible if the attacker overwrites stack variables with attacker-supplied instructions.

As webservers normally run with SYSTEM privileges on Microsoft Windows operating systems, this may result in a full compromise of a host running the vulnerable software.

It should be noted that this unchecked buffer may also be exploited to cause a denial of service condition.

4. FastTrack P2P Technology Message Service Identity Spoofing Vulnerability

BugTraq ID: 4121

Remote: Yes

Date Published: Feb 17 2002 12:00A

Relevant URL:

<http://www.securityfocus.com/bid/4121>

Summary:

KaZaA, Grokster and Morpheus are file-sharing clients based on FastTrack P2P technologies. They will run on Microsoft Windows 9x/ME/NT/2000/XP systems. Ports also exist for variants of the Linux operating system.

Vulnerable file-sharing clients use HTTP to implement a messaging service which allows users of the clients to communicate with each other. However, it is possible for a user to craft a raw fake HTTP GET header to spoof the identity of another existing user. The host and username in the header must both be valid for this to work.

Clients listen for messages on port 1214 by default, even when they are not actively connected to the service.

Any versions of file-sharing clients based on FastTrack P2P technologies which include the messaging functionality should be considered prone to this issue.

This is a security vulnerability because access control is based on client identities, supplied in the request headers.

Attackers may spoof their identity to exploit BugTraq ID 4122 "FastTrack P2P Technology Message Service Denial Of Service Vulnerability".

5. Microsoft Visual C++ 7/Visual C++.Net Buffer Overflow Protection Weakness

BugTraq ID: 4108

Remote: Unknown

Date Published: Feb 14 2002 12:00A

Relevant URL:

<http://www.securityfocus.com/bid/4108>

Summary:

The Microsoft Visual C++ 7 and Visual C++.Net compilers shipped by Microsoft include a feature to help protect against stack-based buffer overflow conditions. The technology is similar to StackGuard, which was developed by Crispin Cowan.

The buffer overflow protection is implemented using special values (called 'security cookies') positioned next to function stack frames when procedures are called. When a procedure exits, the value is checked for its integrity. If the check fails, it is assumed that the value was overwritten due to an overflow condition and either the process terminates or a developer-specified handler executes.

A function pointer for this handler is stored in a global variable. Some overflow conditions may allow for arbitrary addresses to be overwritten. If such a condition exists, an attacker can overwrite the handler variable with a pointer to shellcode. If this is accomplished, the protection mechanism can be circumvented and the shellcode will be executed when the handler function is called.

This is not a vulnerability in itself. This condition is a weakness in the design of this protection mechanism that may lead to a false sense of security.

The perception of security at the compiler level may lead to some programmers using insecure programming techniques.

It should be noted that the weaknesses of similar systems are well documented.

6. FastTrack P2P Technology Message Service Denial Of Service Vulnerability

BugTraq ID: 4122

Remote: Yes

Date Published: Feb 17 2002 12:00A

Relevant URL:

<http://www.securityfocus.com/bid/4122>

Summary:

KaZaA, Grokster and Morpheus are file-sharing clients based on FastTrack P2P technologies. They will run on Microsoft Windows 9x/ME/NT/2000/XP systems. Ports also exist for variants of the Linux operating system.

It has been reported that it is possible to starve resources on a host running a vulnerable client by repeatedly sending messages. Multiple pop-up windows caused by the messages may cause system instability, resulting in a denial of service. The vulnerable software places no reasonable resource limits on the memory that may be consumed by these pop-ups.

While normally this issue could be mitigated by using the features provided by the client to ignore a malicious user who is repeatedly sending messages, it has been discovered that it is also possible for an attacker to spoof their identity.

The identity spoofing issue is described in BugTraq 4121 "FastTrack P2P Technology Message Service Identity Spoofing Vulnerability".

Any versions of file-sharing clients based on FastTrack P2P technologies which include the messaging functionality should be considered prone to this issue.

This issue has reportedly been addressed in KaZaA v1.5.

7. Dino's Webserver Denial of Service Vulnerability

BugTraq ID: 4123

Remote: Yes

Date Published: Feb 18 2002 12:00A

Relevant URL:

<http://www.securityfocus.com/bid/4123>

Summary:

Dino's Webserver is a small web server designed for personal use. It is available for Microsoft Window's based machines. Reportedly, Dino's webserver is subject to a denial of service condition.

Submitting multiple GET requests composed of an unusually long string of arbitrary characters, could cause a host's CPU usage to spike to 100% consuming all available system resources.

A restart of the server may be required in order to regain normal functionality.

This issue may be the result of an unchecked buffer. If this is the case, there is a possibility that arbitrary code may be executed on the vulnerable target. However, this has not yet been confirmed.

8. GNUJSP File Disclosure Vulnerability

BugTraq ID: 4125

Remote: Yes

Date Published: Feb 19 2002 12:00A

Relevant URL:

<http://www.securityfocus.com/bid/4125>

Summary:

GNUJSP is a freely available, open-source implementation of Sun's Java Server Pages. It will run on most Unix and Linux variants, as well as Microsoft Windows NT/2000 operating systems.

A vulnerability has been discovered in GNUJSP which may allow a remote attacker to gain unauthorized access to sensitive information.

It has been reported that a remote attacker may disclose the contents of directories via a specially crafted web request. This may be exploited to list directories, read the contents of arbitrary web-readable files, and disclose script source code. The attacker simply appends the name of the directory and/or file to be disclosed to a web request for /servlets/gnujsp/.

It should be noted that this allow an attacker to circumvent .htaccess files.

This issue may be the result of a configuration error.

9. Multiple Vendor HTTP CONNECT TCP Tunnel Vulnerability

BugTraq ID: 4131

Remote: Yes

Date Published: Feb 19 2002 12:00A

Relevant URL:

<http://www.securityfocus.com/bid/4131>

Summary:

Multiple software and integrated server packages that function as web proxies may be used as open TCP proxies. This is through the usage of the HTTP CONNECT method by default. This method is detailed in RFC 2817, where it is used to build generic Transit Layer Security over HTTP.

Upon receiving a CONNECT request, vulnerable products act as a TCP proxy, tunneling the conversation. This request can target an arbitrary machine inside the firewall, on an arbitrary port. For example, an outside party may request a connection to the internal mail server on port 25.

This functionality may allow communications with any internal machine which will accept connections from the vulnerable server. An attacker may be able to, for instance, use an internal mail server as an open relay for the purposes of sending unsolicited mass email.

In many cases, this behavior may be controlled through the server configuration. Often it is related to support for tunneling or SSL related functionality.

This advisory represents a preliminary list of vendors which may have vulnerable default configurations. Updates will be sent out as additional information becomes available.

III. MICROSOFT FOCUS LIST SUMMARY

1. Security tool (Thread)

Relevant URL:

[http://www.securityfocus.com/cgi-bin/archive.pl?id=88\\$fa46f570\\$bbc7fea9@STEALTH](http://www.securityfocus.com/cgi-bin/archive.pl?id=88$fa46f570$bbc7fea9@STEALTH)

2. Unsigned Windows 2000 Patches (Thread)

Relevant URL:

[F2353Akwt5QztQoPAzd0001250e@hotmail.com//www.securityfocus.com/cgi-bin/archive.pl?id=88href="mailto:F23](http://www.securityfocus.com/cgi-bin/archive.pl?id=88href=)

3. Exchange Security (Thread)

Relevant URL:

SecurityFocus Microsoft: SecurityFocus Microsoft Newsletter #75

<http://www.securityfocus.com/cgi-bin/archive.pl?id=88D411B1A600508B677DEA03F4EA18@MSPNTMAIL>

4. Cached Domain Password on Notebook, secure? (Thread)

Relevant URL:

<LMEDKDLGMAAFJHCJKOIFGENECFAA.alancr@ntlworld.com//www.securityfocus.com/cgi-bin/archive.pl?id=8>

5. restricting permissions for services in Win2K (Thread)

Relevant URL:

[http://www.securityfocus.com/cgi-bin/archive.pl?id=88\\$17153b00\\$0200a8c0@lifelesswks](http://www.securityfocus.com/cgi-bin/archive.pl?id=88$17153b00$0200a8c0@lifelesswks)

6. Restrict Access to drives (Thread)

Relevant URL:

<E8841AEE343308459C615AA653F811CF468C6C@mazenod-mail.mazenod.vic.edu.au//www.securityfocus.com/cgi>

7. quick question... (Thread)

Relevant URL:

<AAEJJLOGDIINFKOLIPEMCEKKCOAA.ken.hoover@yale.edu//www.securityfocus.com/cgi-bin/archive.pl?id=88h>

8. reading data from RAM (Thread)

Relevant URL:

[1e01a8c0@eCompany.gov//www.securityfocus.com/cgi-bin/archive.pl?id=88\\$6f93f7a0\\$1e01a8c0@eCompany.gov](1e01a8c0@eCompany.gov//www.securityfocus.com/cgi-bin/archive.pl?id=88$6f93f7a0$1e01a8c0@eCompany.gov)

9. SecurityFocus Microsoft Newsletter #74 (Thread)

Relevant URL:

<Pine.LNX.4.43.0202191329270.18045-100000@mail.securityfocus.com//www.securityfocus.com/cgi-bin/archive.pl?>

10. Extra Encryption On SAM file other than md4 and syskey (Thread)

Relevant URL:

<5.1.0.14.2.20020218171142.00a259f0@mail.tsn.cc//www.securityfocus.com/cgi-bin/archive.pl?id=88href="mailto:5.1>

11. FW: reading data from RAM (Thread)

Relevant URL:

<http://www.securityfocus.com/cgi-bin/archive.pl?id=88D311B948009027D3B1A1ECE559@ntserv05>

12. SQL SA password (Thread)

Relevant URL:

<200202162256.AA256639184@nocmail3.itxc.net//www.securityfocus.com/cgi-bin/archive.pl?id=88href="mailto:200>

13. How to turn on the Macro prompt on MS Of (Thread)

Relevant URL:

<E748F5C5A5A8D411B14100508BDCB15CD7FCBB@mail.mis.sandstream.com//www.securityfocus.com/cgi-bin/ar>

14. Windows CE (Thread)

Relevant URL:

[http://www.securityfocus.com/cgi-bin/archive.pl?id=88\\$998064e0\\$6be23544@dafcosfc75w8ry](http://www.securityfocus.com/cgi-bin/archive.pl?id=88$998064e0$6be23544@dafcosfc75w8ry)

15. RFC (Thread)

Relevant URL:

<E748F5C5A5A8D411B14100508BDCB15CD7FCB8@mail.mis.sandstream.com/www.securityfocus.com/cgi-bin/ar>

IV. NEW PRODUCTS FOR MICROSOFT PLATFORMS

1. SafeWord

by Secure Computing

Platforms: UNIX, Solaris, Windows NT, SunOS, AIX, HP-UX, BSDI

Relevant URL:

<http://www.securecomputing.com/index.cfm?sKey=643>

Summary:

SafeWord Plus from Secure Computing is a complete, out-of-the-box solution for user authentication, authorization, and accountability (AAA) for both PKI and non-PKI applications. Easy to install and manage, SafeWord Plus offers powerful administrative features, such as role-based access control and user self-enrollment, integrated with an LDAP-based directory.

2. SoftClan e-cryptor

by CenturionSoft

Platforms: Windows 95/98, Windows NT, Windows 2000, Windows XP

Relevant URL:

<http://www.centurionsoft.com/SoftClan/ecryptor.htm>

Summary:

SoftClan e-cryptor is unique in that it offers both powerful AES encryption as well as ease-of-use. Encrypted files are self-decrypting. Your encrypted email recipients need nothing to decrypt the file except the password. E-cryptor is also perfect for encrypting files and folders because you never have to worry about having the software installed to decrypt them. This is particularly helpful if you want to encrypt files; including backup files – on removable media. You can decrypt them on any system, even a system that doesn't have e-cryptor installed.

3. Norton Internet Security 2002

by Symantec

Platforms: Windows 95/98

Relevant URL:

<http://www.symantec.com/sabu/nis/index.html>

Summary:

Comprehensive Security Suite Norton Internet Security is the first security suite that is available for home PC users and small businesses. Norton Internet Security is an integrated and comprehensive suite that

combines different technologies to address all of the major security threats for maximum online protection.

4. WebAgain

by LOCKSTEP SYSTEMS, INC.

Platforms: Windows NT, Windows 2000

Relevant URL:

<http://www.lockstep.com/products/webagain/wa-product.html>

Summary:

WebAgain automatically detects when an unauthorized change has been made to your web site and republishes the appropriate information in seconds – without taking your web site offline. WebAgain is the only utility that concentrates on repairing web site damage, in addition to sending a notification when a hack has been detected.

V. NEW TOOLS FOR MICROSOFT PLATFORMS

1. File::Scan v0.05

by Henrique Dias hdias@aeiou.pt

Relevant URL:

<http://www.cpan.org/authors/id/H/HD/HDIAS/>

Platforms: N/A

Summary:

File::Scan allows users to make multiplatform virus scanners which can detect Windows/DOS/Mac viruses. It include a virus scanner and signatures database.

2. MIMEDefang v2.5

by David F. Skoll dfs@roaringpenguin.com

Relevant URL:

<http://www.roaringpenguin.com/mimedefang/>

Platforms: Linux, Perl (any system supporting perl), UNIX

Summary:

MIMEDefang is a flexible MIME e-mail scanner designed to protect Windows clients from viruses. It can alter or delete various parts of a MIME message according to a very flexible configuration file. It can also bounce messages with unacceptable attachments. MIMEDefang works with Sendmail 8.11's new "Milter" API, which gives it much more flexibility than procmail-based approaches.

3. nmbscan v1.2.1

by Gregoire Barbier

Relevant URL:

<http://gbarbier.free.fr/prj/dev/#nmbscan>

Platforms: POSIX

Summary:

NMB Scanner scans the shares of a SMB network, using the NMB and SMB protocols. It is useful for acquiring information on a local area network for such purposes as security auditing. It can obtain such information as NMB/SMB/Windows hostname, IP address, IP hostname, ethernet MAC address, Windows username, NMB/SMB/Windows domain name, and master browser. It can discover all the NMB/SMB/Windows hosts on a local area network by using the hosts lists maintained by master browsers.

VI. SPONSORSHIP INFORMATION

This Issue is Sponsored by: Stonesoft Inc.

Stonesoft is among the most trusted names in high availability software designed to reinforce all market-leading firewalls. Today, StoneBeat® FullCluster(TM) is the only high availability solution that enhances Microsoft's Internet Security & Acceleration Server with fault-tolerance and transparent failover, network-level scalability, and true dynamic load balancing.

To learn more, visit our Web site at:

<http://www.stonesoft.com/products/main/isa>

or Call 866-869-4075 or contact us at ISAServer@stonesoftcom.

- **Previous message:** [Steele John J9C658: "Info:NT/Win2k"](#)
- **Messages sorted by:** [\[date \]](#) [\[thread \]](#) [\[subject \]](#) [\[author \]](#) [\[attachment \]](#)