

# SecurityFocus Microsoft Newsletter #90

**Source:** <http://www.derkeiler.com/Mailing-Lists/securityfocus/focus-ms/2002-06/0041.html>

---

**From:** Marc Fossi ([mfossi@securityfocus.com](mailto:mfossi@securityfocus.com))

**Date:** 06/11/02

Date: Mon, 10 Jun 2002 16:19:33 -0600 (MDT)  
From: Marc Fossi <[mfossi@securityfocus.com](mailto:mfossi@securityfocus.com)>  
To: Focus-MS <[focus-ms@securityfocus.com](mailto:focus-ms@securityfocus.com)>

SecurityFocus Microsoft Newsletter #90

---

This newsletter is sponsored by SecurityFocus ([www.securityfocus.com](http://www.securityfocus.com))

Attention Non-profits and Universities: Sign-up now for preferred pricing on the only global early-warning system for cyber attacks – SecurityFocus ARIS Threat Management System.

Click here for more info

<http://www.securityfocus.com/corporate/products/pdpsection.shtml>

---

## I. FRONT AND CENTER

1. Optimizing NIDS Performance
2. XP Professional Security Features: An Introduction
3. A Virus by Any Other Name: Virus Naming Practices
4. Black Hat Briefings & Training

## II. MICROSOFT VULNERABILITY SUMMARY

1. Evolvable Shambala Server FTP Server Directory Traversal...
2. Evolvable Shambala Server Web Server Denial Of Service...
3. University Of Washington IMAP Arbitrary File Access Vulnerability
4. Working Resources BadBlue Directory Contents Disclosure...
5. Teekai's Tracking Online Cross-Site Scripting Vulnerability
6. Microsoft Internet Explorer Gopher Client Buffer Overflow...

## III. MICROSOFT FOCUS LIST SUMMARY

1. SQL 7.0 SP3 Missing Setup.exe (Thread)
2. SMTP authentication (w2k SMTP service) (Thread)
3. Comments/suggestions..TIA (Thread)
4. Power Users vs. Restricted user – Win2000 (Thread)
5. Workstation security question (Thread)
6. Assistance Needed (Thread)
7. Administrivia (Thread)
8. Phantom connections to 216.37.13.59 & .196 (Thread)
9. SecurityFocus Microsoft Newsletter #89 (Thread)

10. SBS 2000 accounts security settings (Thread)

#### IV. MICROSOFT PRODUCTS

1. i.Secure Store
2. ProBot software
3. AiS AliveProxy Professional

#### V. MICROSOFT TOOLS

1. Network Equipment Performance Monitor v0.90b1
2. Advanced Net Tools (ANT) 2.7
3. Archaeopteryx v1.0
4. Folder Guard

#### VI. SPONSORSHIP INFORMATION

##### I. FRONT AND CENTER

-----

###### 1. Optimizing NIDS Performance

By Neil Desai

To help network intrusion detection systems keep up with the demands of today's networks, and the wide variety of threats that besiege them, there are a number of things that the NIDS administrator can do to improve the performance of their NIDS. This article will examine some of those options.

<http://online.securityfocus.com/infocus/1589>

###### 2. XP Professional Security Features: An Introduction

by Timothy M. Mullen

I'm not sure if it was the uplifting backbeat of Madonna's "Ray of Light" or the promise of the best security options yet in a Microsoft operating system that made the difference, but the overall development and marketing efforts of XP have paid off. With over 32 millions copies sold since it was released last October, Microsoft's newest line of operating system products has caught the attention of both home and business users.

<http://online.securityfocus.com/infocus/1588>

###### 3. A Virus by Any Other Name: Virus Naming Practices

by Costin Raiu, Kaspersky Labs Romania

When the "VBS/VBSWG.J" virus appeared, the media decided to call it by a more appealing name, "AnnaKournikova", which was derived from the JPEG file that the virus claimed to be. However, none of the anti-virus products included in the excellent virus names cross reference tool VGrep currently lists this virus as "AnnaKournikova", "Kournikova", or any other variation based on the name of the charismatic tennis player. On the other hand, a considerable number of AV programs detect it as "SST", while a very small number don't call it "VBSWG" or "SST".

<http://online.securityfocus.com/infocus/1587>

#### 4. Black Hat Briefings & Training

Attend Black Hat Briefings & Training, July 29 – August 1, Las Vegas, the world's premier technical security event! 8 tracks, 12 training sessions, Richard Clarke keynote, 500 delegates from 30 nations, with a near cult following of both CSOs and "underground" security experts. See for yourself what the buzz is all about.

Please visit [www.blackhat.com](http://www.blackhat.com) for more information.

## II. BUGTRAQ SUMMARY

---

### 1. Evolvable Shambala Server FTP Server Directory Traversal Vulnerability

BugTraq ID: 4896

Remote: Yes

Date Published: May 31 2002 12:00A

Relevant URL:

<http://www.securityfocus.com/bid/4896>

Summary:

Shambala Server is a FTP, Web, and Chat server targeted for the Small Office/Home Office user. It has been designed for use with Microsoft Windows operating systems.

It has been reported that Shambala Server's FTP server is vulnerable to a directory traversal condition. By using directory traversal sequences (ie './.', '..'), an attacker can obtain files outside of the permitted directory structure.

Disclosure of sensitive files and the filesystem layout may supply an attacker with important information. This information could lead to further compromise of the vulnerable system.

### 2. Evolvable Shambala Server Web Server Denial Of Service Vulnerability

BugTraq ID: 4897

Remote: Yes

Date Published: May 31 2002 12:00A

Relevant URL:

<http://www.securityfocus.com/bid/4897>

Summary:

Shambala Server is a FTP, Web, and Chat server targeted for the Small Office/Home Office user. It has been designed for use with Microsoft Windows operating systems.

It has been reported that Shambala Server's web server may be prone to a denial of service vulnerability. The denial of service condition is a result of the web server failing to handle malformed requests.

Reportedly, exploiting this condition will cause the web server to return a "Run-time error'5': Invalid procedure call or argument" failure. This

will cause the web server to crash and causing the denial of service condition.

### 3. University Of Washington IMAP Arbitrary File Access Vulnerability

BugTraq ID: 4909

Remote: Yes

Date Published: Jun 01 2002 12:00A

Relevant URL:

<http://www.securityfocus.com/bid/4909>

Summary:

uw-imap is an open source Internet Message Access Protocol daemon. It is distributed and maintained by the University of Washington, and available for most operating systems including Unix, Linux, and Microsoft Windows.

A feature in the daemon may make it possible for users to gain access to unauthorized information.

By default, uw-imap allows users to view files on the system on which the daemon runs. The daemon allows users to view files that are normally readable through a shell on the system with equivalent user privileges.

In configurations where users are not authorized shell access to a system, but have a valid account from which to download mail via IMAP, a user may be able to gain access to information on the server. The feature enabled by default that allows users to view files via the IMAP daemon could result in information leakage on systems that depend on users not being able to view files on the local system.

Disabling this feature on Microsoft Windows systems may present additional problems. By design, the software does not filter the '\\' symbol.

This could result in leakage of potentially sensitive information to an unauthorized user. It should be noted that this feature is not documented in the literature distributed with the software.

### 4. Working Resources BadBlue Directory Contents Disclosure Vulnerability

BugTraq ID: 4912

Remote: Yes

Date Published: Jun 03 2002 12:00A

Relevant URL:

<http://www.securityfocus.com/bid/4912>

Summary:

Working Resources BadBlue is a webserver intended to share various resources and is developed for Microsoft Windows environments. By default BadBlue prevents users from viewing the contents of directories.

It has been reported that version 1.7.0 of BadBlue discloses the contents of directories when a certain character is present.

If a remote user appends the unicode variant of the "%" (0x25) symbol, it will cause the web server to display the contents of the current directory.

The information obtained may be used by an attacker for further attacks against a vulnerable system.

#### 5. Teekai's Tracking Online Cross-Site Scripting Vulnerability

BugTraq ID: 4924

Remote: Yes

Date Published: Jun 03 2002 12:00A

Relevant URL:

<http://www.securityfocus.com/bid/4924>

Summary:

Teekai's Tracking Online is a script for tracking website usage. It is written in PHP and will run on most Unix and Linux variants as well as Microsoft Windows operating systems.

Teekai's Tracking Online does not adequately filter HTML tags from certain URL parameters, making it prone to cross-site scripting attacks.

Attackers may exploit this by creating a malicious link to a vulnerable webpage. When a web user visits the malicious link, the attacker's script code will be executed in their browser in the security context of the website running the Tracking Online software.

#### 6. Microsoft Internet Explorer Gopher Client Buffer Overflow Vulnerability

BugTraq ID: 4930

Remote: Yes

Date Published: Jun 04 2002 12:00A

Relevant URL:

<http://www.securityfocus.com/bid/4930>

Summary:

Microsoft Internet Explorer includes a gopher client. Reportedly, this client is vulnerable to a buffer overflow condition. This vulnerability was reported to exist in versions 5.5 and 6.0 of Microsoft Internet Explorer.

The condition is present when MSIE parses gopher server replies. A malicious gopher server may be able to return a gopher reply that will exploit the overflow and run arbitrary code on a user's system.

An attacker may exploit this issue to crash a web user's browser or to execute supplied code. This is most likely to occur via a hyperlink in a malicious webpage, but may also occur via HTML e-mail.

It is not known if other versions of Microsoft Internet Explorer are vulnerable to this issue.

### III. MICROSOFT FOCUS LIST SUMMARY

---

1. SQL 7.0 SP3 Missing Setup.exe (Thread)

Relevant URL:

[5.1.1.2.2.20020606174214.01bdab58@mail.emarket2.com](http://online.securityfocus.com/archive/88/5.1.1.2.2.20020606174214.01bdab58@mail.emarket2.com)">http://online.securityfocus.com/archive/88/5.1.1.2.2.2002

2. SMTP authentication (w2k SMTP service) (Thread)

Relevant URL:

<http://online.securityfocus.com/archive/88/VPOP31.5.4.20020606155859.390.47.1.252514d7@server>

3. Comments/suggestions..TIA (Thread)

Relevant URL:

[7092733AEB68D41191940008C79F1574012426C9@ATL0NTS-EXCH.rzim.org](http://online.securityfocus.com/a7092733AEB68D41191940008C79F1574012426C9@ATL0NTS-EXCH.rzim.org)">http://online.securityfocus.com/a

4. Power Users vs. Restricted user – Win2000 (Thread)

Relevant URL:

[http://online.securityfocus.com/archive/88/00ae01c20cae\\$70c53390\\$11e060a@rippin](http://online.securityfocus.com/archive/88/00ae01c20cae$70c53390$11e060a@rippin)

5. Workstation security question (Thread)

Relevant URL:

[29229974636.20020605083824@planb-security.net](http://online.securityfocus.com/archive/88/29229974636.20020605083824@planb-security.net)">http://online.securityfocus.com/archive/88/29229974636.20020

6. Assistance Needed (Thread)

Relevant URL:

[E00ECDDED326C0B4288A0B4F7F02DE2DD131BE5@mickey.quest.fl.com](http://online.securityfocus.com/archive/E00ECDDED326C0B4288A0B4F7F02DE2DD131BE5@mickey.quest.fl.com)">http://online.securityfocus.com/archive

7. Administrivia (Thread)

Relevant URL:

[Pine.LNX.4.43.0206040753240.19598-100000@mail.securityfocus.com](http://online.securityfocus.com/archive/88/Pine.LNX.4.43.0206040753240.19598-100000@mail.securityfocus.com)">http://online.securityfocus.com/archive/88/

8. Phantom connections to 216.37.13.59 & .196 (Thread)

Relevant URL:

[http://online.securityfocus.com/archive/88/00ef01c20b43\\$144c1500\\$97d14a81@naomi](http://online.securityfocus.com/archive/88/00ef01c20b43$144c1500$97d14a81@naomi)

9. SecurityFocus Microsoft Newsletter #89 (Thread)

Relevant URL:

[Pine.LNX.4.43.0206031453160.27478-100000@mail.securityfocus.com](http://online.securityfocus.com/archive/88/Pine.LNX.4.43.0206031453160.27478-100000@mail.securityfocus.com)">http://online.securityfocus.com/archive/88/

10. SBS 2000 accounts security settings (Thread)

Relevant URL:

[3C1E3607B37295439F7C409EFBA08E68022EDCA9@US-Columbia-CIST.mail.saic.com](http://online.securityfo3C1E3607B37295439F7C409EFBA08E68022EDCA9@US-Columbia-CIST.mail.saic.com)">http://online.securityfo

#### IV. NEW PRODUCTS FOR MICROSOFT PLATFORMS

---

##### 1. i.Secure Store

by Archisoft Security Solutions Limited

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

Relevant URL:

<http://www.archisoft.com.hk/prod02.htm>

Summary:

i.Secure Store is a plug-in security module for Microsoft Windows. It makes use of the latest PKI technology together with personal Smart Token to ensure that every information that reaches its users is uniquely identified, confidential and intact. i.Secure Store works transparently with Microsoft Windows to promote supreme security

##### 2. ProBot software

by NetHunter Group

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

Relevant URL:

<http://www.nethunter.cc/probot.php>

Summary:

ProBot is a powerful workstation monitoring solution. This software generates the detailed event log that is kept securely in binary files. These files may be later referred by the system administrator or computer owner for the exact reconstruction of the computer usage.

##### 3. AiS AliveProxy Professional

by AtomInterSoft

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

Relevant URL:

<http://www.atomintersoft.com/products/alive-proxy/>

Summary:

AiS AliveProxy Pro extracts proxy servers addresses from specified Internet pages, or files, checks the type (transparent or anonymous), and measures connection speed, tracerout and timeout. Result of its work is a list of "alive" proxies, without duplicates. High-efficiency multy-threaded engine allow you to check more than 100 proxy per second. High-speed export proxy from URLs or files. Export/Import data from/to XML, Excel, TXT, HTML, RTF

#### V. MICROSOFT TOOLS

---

##### 1. Network Equipment Performance Monitor v0.90b1

by jimesh

Relevant URL:

<http://www.nepm.net/>

Platforms: AIX, FreeBSD, HP-UX, Linux, Solaris, True64 UNIX, UNIX, Windows 2000, Windows NT, Windows XP

Summary:

NEPM monitors and reports uptime, critical events and their predecessors, access rates, bytes-served rates, and error rates for network node equipment. Hardware and software elements within the nodes are tracked and reported separately to make possible rapid fault isolation. It is a very general, highly configurable, two-part software system that captures and analyzes logged performance data from IP-networked equipment and reports it via email and Web pages. Current conditions and history from systems based on Windows NT/2000, Unix, and Unix-style operating systems can be tracked and reported. Most major server, switch and router systems can be monitored, without running agents on the target systems. NEPM itself is system-independent and can be hosted on either a Unix or Win NT system or a combination of these with equal ease.

## 2. Advanced Net Tools (ANT) 2.7

by Mikersoft

Relevant URL:

<http://www.mikersoft.com/ant/anttrial.zip>

Platforms: Windows 2000, Windows 95/98

Summary:

Share Scanner can scan any network for a list of shared drives. ARP Configuration allows you to add/remove ARP entries and view the ARP table all from a Windows GUI. Route Configuration allows you to add/remove Routing entries and view the route table all from a Windows GUI. Adapter Configuration allows you to view all adapters and add remove IP addresses of individual adapters using a Windows GUI. IP Configuration shows you all of the configuration information for all of the adapters on your system. Net Stats shows all of the current connections on your PC and their current state. It also shows what ports applications are listening on. You can set the refresh rate at any speed you wish. TraceRoute tells you how many hops (routers) are between your PC and another destination. It will also show you the slowest connection point. Network Scanner can scan any class A, B or C network for any list of open ports. Network Scanner takes advantage of multi-threading. You can use many threads to scan at the same time for quick results. You can save your port list to a text file. You can also save your list of found connections to a text file. Port Scanner can scan any computer for a list, or range of open ports. Set your speed of finding open ports by setting the timeout variable. Ping Utility allows you to change the size of the packets, the timeout, and the number of packets to ping. Advanced DNS Utility shows you extended information on a given hostname or IP address. You can also lookup the mail exchange servers, or domain name servers for a specific domain. Query types available: A, ANY, NS, MX, SOA. Command Test, a utility for connecting to an open port and testing commands. Works like a telnet client but you can send 1 line at a time. Whois Client where you can configure the whois server for multiple DNS name types. With ANT you don't even need to use the main GUI interface, all menus are accessible from the system tray icon.

## 3. Archaeopteryx v1.0

by FoxThree

Relevant URL:

<http://members.fortunecity.com/sektorsecurity/projects/archaeopteryx.html>

Platforms: Windows 2000, Windows NT

Summary:

Archaeopteryx is a Passive mode OS Identification Tool. It is based off Siphon v.666 by SubTerrain. It has a great GUI and a highly configurable OS signature file. It uses POSIX threads for multi-threading (pthreads for Win32). Also requires WinPCAP Drivers. We plan to support this tool actively! So, please send all new OS signatures to us

#### 4. Folder Guard

by WinAbility

Relevant URL:

<http://www.winability.com>

Platforms: Windows 95/98, Windows NT

Summary:

Folder Guard allows you to selectively hide files, folders and restrict access to other resources. Makes folders invisible to any application, including Explorer, MS Office, MS-DOS prompt, common dialogs, etc. Provides password protection, user-dependent configurations. Highly customizable and user friendly. For personal systems or corporate networks.

## VI. SPONSORSHIP INFORMATION

---

This newsletter is sponsored by SecurityFocus ([www.securityfocus.com](http://www.securityfocus.com))

Attention Non-profits and Universities: Sign-up now for preferred pricing on the only global early-warning system for cyber attacks – SecurityFocus ARIS Threat Management System.

Click here for more info

<http://www.securityfocus.com/corporate/products/pdpsection.shtml>

---

- **Previous message:** [Kit: "RE: Windows Reverification"](#)
- **Messages sorted by:** [\[ date \]](#) [\[ thread \]](#) [\[ subject \]](#) [\[ author \]](#) [\[ attachment \]](#)