

# SecurityFocus Microsoft Newsletter #51

*Source:* <http://www.derkeiler.com/Mailing-Lists/securityfocus/focus-ms/2001-09/0050.html>

---

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

**Date:** 09/10/01

Date: Mon, 10 Sep 2001 15:58:34 -0600 (MDT)  
From: Marc Fossi <[mfossi@securityfocus.com](mailto:mfossi@securityfocus.com)>  
To: Focus-MS <[focus-ms@securityfocus.com](mailto:focus-ms@securityfocus.com)>  
Subject: SecurityFocus Microsoft Newsletter #51  
Message-ID: <Pine.GSO.4.30.0109101557590.1844-100000@mail>

SecurityFocus Microsoft Newsletter #51

---

This Issue Sponsored by: Foundstone

"Ultimate Hacking: Hands On – NT/2000 Security"

If you're running a Windows network, then this is the intensive 3-day course with everything a hacker knows...that you'll need to know! As a Specialist in Microsoft's Security Services Partner Program, Foundstone knows hacking, security and Microsoft. Register now for the class in New York City, September 25–27 and Irvine, CA December 11–13.

<http://www.foundstone.com/NT>

---

## I. FRONT AND CENTER

1. Chasing the Wind, Episode 10: the Road Less Traveled
2. 'Good' viruses have a future
3. Virtual Private Networks: A Broken Dream?

## II. MICROSOFT VULNERABILITY SUMMARY

1. Microsoft Outlook Web Access Denial of Service Vulnerability
2. Outlook Express 6 Attachment Security Bypass Vulnerability

## III. MICROSOFT FOCUS LIST SUMMARY

1. What does 128-bit support for W2K give me? (Thread)
2. Insufficient port error (Thread)
3. All Services Disabled? (Thread)
4. Windowsupdate.microsoft.com / Wondering. (Thread)
5. %u encoding IDS bypass vulnerability (Thread)
6. alternate data stream... (Thread)
7. NT disk scanning ... (Thread)
8. Securing W2Kpro – ACLs? (Thread)
9. SecurityFocus Microsoft Newsletter #50 (Thread)
10. ARIS Analyzer Version 1.5 (Thread)

11. R: Windowsupdate.microsoft.com – getting updates manually...
12. Way to read Exchange 2000 database files (Thread)
13. Audit Tools (Thread)

#### IV. NEW PRODUCTS FOR MICROSOFT PLATFORMS

1. Digitivity CAGE
2. Anti-Virus Toolkit for Microsoft Exchange
3. Exceleration PolicyWare
4. Storage Management
5. Advanced Outlook Express Password Recovery
6. Symantec Norton Internet Security 2001

#### V. NEW TOOLS FOR MICROSOFT PLATFORMS

1. Typhon
2. Winfingerprint v0.3.0
3. rain v1.2.8r2
4. Anubis
5. MacAnalysis 2.0b

#### VI. SPONSORSHIP INFORMATION

##### I. FRONT AND CENTER

---

1. Chasing the Wind, Episode 10: the Road Less Traveled  
by Robert G. Ferrell

This is the tenth installment of SecurityFocus's popular Chasing the Wind series. In the last episode, we left Jake in the middle of his five-day hacking seminar and Douglas continued to forge ahead on the mysterious Bellatrix Project. Meanwhile, unbeknownst to Douglas or to the United States department of Defence, the shady figure known only as "Baseball Cap" was successfully monitoring the Bellatrix project.

<http://www.securityfocus.com/focus/ih/articles/chasing10.html>

2. 'Good' viruses have a future  
by Shane Coursen

Should we fight viruses with more viruses? Mad cyber-scientists have made the moral question moot.

<http://www.securityfocus.com/templates/column.html?id=23>

3. Virtual Private Networks: A Broken Dream?  
by Eric Hines

Virtual Private Networks allow organizations to establish secure links with business partners and extend communications to regional and isolated offices. In doing so, they significantly diminish the cost of communications for an increasingly mobile workforce. While VPNs are gaining widespread acceptance as security solutions, they are not a panacea. This article will serve as a brief introduction to VPN technology. It will also illustrate some vulnerabilities that have been discovered in VPNs.

<http://www.securityfocus.com/focus/basics/articles/vpn.html>

## II. BUGTRAQ SUMMARY

-----

### 1. Microsoft Outlook Web Access Denial of Service Vulnerability

BugTraq ID: 3223

Remote: Yes

Date Published: 2001-08-22

Relevant URL:

<http://www.securityfocus.com/bid/3223>

Summary:

Outlook Web Access is an optional component of Microsoft Exchange Server which runs in conjunction with Microsoft Internet Information Server. It provides access to a user's Exchange mailbox through a web interface.

A user can enter a long string of % characters into the Log On field in the Outlook Web Access logon page. Next, the NT challenge dialog will pop up requesting the username and password. The user enters the same long string into both the username and password fields and presses <enter> until the request times out.

At this point both the WWW Publishing service and the IIS Administration service are stopped. This results in the inability of the host server to fulfill HTTP requests or start the IIS Administration interface.

An administrator must manually restart the services to resume normal operation of the server.

Note: If this behaviour is due to a buffer overrun condition, it may be possible to execute arbitrary code on the server with administrative privileges.

### 2. Outlook Express 6 Attachment Security Bypass Vulnerability

BugTraq ID: 3271

Remote: No

Date Published: 2001-08-30

Relevant URL:

<http://www.securityfocus.com/bid/3271>

Summary:

Microsoft Outlook Express 6 contains a new security feature which prevents users from opening potentially harmful file attachments. File extensions filtered by this feature are those which generally can be used to carry a virus payload.

When the file attachment security feature is turned on, any file attachment type which could potentially carry a virus is unavailable to the recipient to either open or save.

A vulnerability exists which allows a file embedded within an HTML frame in an email message to bypass the dangerous file attachment type security feature. When a message containing an attachment embedded in this way is opened or previewed, the user is automatically prompted to open or save the attachment.

If the user attempts to open the file immediately, the action will fail. However, an assembler coded .exe attachment which has had it's extension changed to .bat will execute immediately. Regardless of the extension type, the user is able to save the attachment to disk.

### III. MICROSOFT FOCUS LIST SUMMARY

---

1. What does 128-bit support for W2K give me? (Thread)

Relevant URL:

[f701fe0a@commtouch.com](http://www.securityfocus.com/frames/index.html?content=%2ftemplates%2farchive.pike%3f701fe0a@commtouch.com)">http://www.securityfocus.com/frames/index.html?content=%2ftemplates%2farchive.pike

2. Insufficient port error (Thread)

Relevant URL:

<http://www.securityfocus.com/frames/index.html?content=%2ftemplates%2farchive.pike%3flist%3d88%26date%3d20000601>

3. All Services Disabled? (Thread)

Relevant URL:

<http://www.securityfocus.com/frames/index.html?content=%2ftemplates%2farchive.pike%3flist%3d88%26date%3d20000601>

4. Windowsupdate.microsoft.com / Wondering. (Thread)

Relevant URL:

[6400000a@internal.home.blockdev.net](http://www.securityfocus.com/frames/index.html?content=%2ftemplates%2farchive.pike%3f6400000a@internal.home.blockdev.net)">http://www.securityfocus.com/frames/index.html?content=%2ftemplates%2f

5. %u encoding IDS bypass vulnerability (Thread)

Relevant URL:

<http://www.securityfocus.com/frames/index.html?content=%2ftemplates%2farchive.pike%3flist%3d88%26date%3d20000601>

6. alternate data stream... (Thread)

Relevant URL:

<http://www.securityfocus.com/frames/index.html?content=%2ftemplates%2farchive.pike%3flist%3d88%26date%3d20000601>

7. NT disk scanning ... (Thread)

Relevant URL:

<http://www.securityfocus.com/frames/index.html?content=%2ftemplates%2farchive.pike%3flist%3d88%26date%3d20000601>

8. Securing W2Kpro – ACLs? (Thread)

Relevant URL:

## SecurityFocus Microsoft: SecurityFocus Microsoft Newsletter #51

[2300a8c0@lauradominion.com">http://www.securityfocus.com/frames/index.html?content=%2ftemplates%2farchive.](http://www.securityfocus.com/frames/index.html?content=%2ftemplates%2farchive.2300a8c0@lauradominion.com)

9. SecurityFocus Microsoft Newsletter #50 (Thread)

Relevant URL:

<http://www.securityfocus.com/frames/index.html?content=%2ftemplates%2farchive.pike%3flist%3d88%26date%3d20>

10. ARIS Analyzer Version 1.5 (Thread)

Relevant URL:

<http://www.securityfocus.com/frames/index.html?content=%2ftemplates%2farchive.pike%3flist%3d88%26date%3d20>

11. R: Windowsupdate.microsoft.com – getting updates manually (Thread)

Relevant URL:

<http://www.securityfocus.com/frames/index.html?content=%2ftemplates%2farchive.pike%3flist%3d88%26date%3d20>

12. Way to read Exchange 2000 database files (Thread)

Relevant URL:

<http://www.securityfocus.com/frames/index.html?content=%2ftemplates%2farchive.pike%3flist%3d88%26date%3d20>

13. Audit Tools (Thread)

Relevant URL:

[0100a8c0@DaemonLabs.com">http://www.securityfocus.com/frames/index.html?content=%2ftemplates%2farchive.p](http://www.securityfocus.com/frames/index.html?content=%2ftemplates%2farchive.0100a8c0@DaemonLabs.com)

### IV. NEW PRODUCTS FOR MICROSOFT PLATFORMS

#### 1. Digitivity CAGE

by Digitivity

Platforms: Solaris and Windows NT

Relevant URL:

<http://www.securityfocus.com/templates/product.html?id=244>

Summary:

The Digitivity CAGE is the first Applet Management System product to be released. Its features include: Routing of Java applets to a server outside the firewall, Central hosting of Java applets in a server environment, Remote displaying of applets, Central control and management, Logging and Dynamic checking.

#### 2. Anti-Virus Toolkit for Microsoft Exchange

by Dr Solomon

Platforms: Windows 95/98 and Windows NT

Relevant URL:

<http://www.securityfocus.com/templates/product.html?id=73>

Summary:

Complete anti-virus protection for Microsoft Exchange, Server and Client. Dr Solomon's Anti-Virus Toolkit automatically scans each e-mail message

and attachment, leaving virus-free files undisturbed. All infected files are immediately isolated or disinfected and forwarded using Dr Solomon's award winning anti-virus engine.

### 3. Excecleration PolicyWare

by NetBoost

Platforms: Windows NT

Relevant URL:

<http://www.securityfocus.com/templates/product.html?id=897>

Summary:

NetBoost's PolicyWare provides a new platform for building and deploying an emerging breed of network policy enforcement applications that address the complexities of today's corporate networks. Network policy enforcement applications translate business policies into network behavior and include firewall, intrusion detection, VPN, RMON probe, rate shaping, and web caching systems.

NetBoost partners with leading vendors of policy enforcement applications and platforms to create flexible, scalable solutions that make today's high-speed corporate networks more efficient, controllable and intelligent. NetBoost provides significant time to market and performance advantages for ISVs and network equipment manufacturers, offering the flexibility of software development with the high-speed performance of custom silicon.

In implementation, NetBoost PolicyWare solutions allow CIOs, network security managers, and network administrators to deploy, update, and enforce network policies more efficiently, as well as, maximize the performance of policy enforcement applications and platforms.

### 4. Storage Management

by St. Bernard Software

Platforms: Windows 2000 and Windows NT

Relevant URL:

<http://www.securityfocus.com/templates/product.html?id=1407>

Summary:

Open File Manager is a utility that enables your existing backup software to successfully capture open files – even if they are changing during the backup. There is no need to close applications or lock out users. With Open File Manager you can run your backup at anytime – all without any interruption to users.

### 5. Advanced Outlook Express Password Recovery

by Elcom Ltd.

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

Relevant URL:

<http://www.securityfocus.com/templates/product.html?id=1463>

Summary:

A program to recover server name, login and password for all mail and news accounts in Microsoft Outlook Express, as well as passwords to "identities". Passwords are recovered instantly, multilingual ones are supported. Works with all versions of Outlook Express.

6. Symantec Norton Internet Security 2001

by Symantec

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

Relevant URL:

<http://www.securityfocus.com/templates/product.html?id=1449>

Summary:

Norton Personal Firewall 2001 v3.0 is your maximum defense against hackers. This powerful software monitors all Internet connections to and from your computer and alerts you to attempted intrusions—including port scans. Automatically block any system trying to probe your PC, as well as prevent personal data from being sent to web sites without your knowledge. And a new Security Assistant makes the software easier than ever to use. Whether your Internet connection is always on or you dial in occasionally, your PC could be in jeopardy.

## V. NEW TOOLS FOR MICROSOFT PLATFORMS

---

1. Typhon

by Next Generation Security Software Ltd

Relevant URL:

<http://www.securityfocus.com/tools/2195>

Platforms: Windows 2000 and Windows NT

Summary:

Typhon, an updated version of Cerberus Internet Scanner, is a vulnerability assessment tool. It will scan a given host for known security holes and vulnerabilities. It does this by looking at the services offered by a host and each of these are examined for holes. For example, Typhon will check for over 180 known vulnerabilities in the web service or daemon offered by a server. Once a scan has been completed a report in HTML is produced detailing what security holes were found, the impact of those holes and how to fix them. Once these holes have been removed then the host will be more secure against attacks. As new vulnerabilities are discovered almost on a daily basis it is necessary to ensure that the Typhon is kept up to date and hosts are scanned on a regular basis.

2. Winfingerprint v0.3.0

by Kirby Kuehl, [vacuum@technotronic.com](mailto:vacuum@technotronic.com)

Relevant URL:

<http://www.securityfocus.com/tools/1291>

Platforms: Windows 2000 and Windows NT

Summary:

Determines OS using SMB Queries, TCP Portscan, ICMP Scan, IP Address Range support, Enumerates NetBIOS Shares, Users, Services, Transports, Sessions, Service Pack and Hotfix Level, Groups and Disks.

3. rain v1.2.8r2

by Evil ([mystic@tenebrous.com](mailto:mystic@tenebrous.com))

Relevant URL:

<http://www.securityfocus.com/tools/2098> >

Platforms: Windows 3.x

Summary:

rain is powerful tool for testing stability of hardware and software utilizing IP protocols. It offers its users the capability of creating their own packets with a wide variety of command line options.

4. Anubis

by The Anubis Team <[ghostface@lodz.pdi.net](mailto:ghostface@lodz.pdi.net)>

Relevant URL:

<http://www.securityfocus.com/tools/2192>

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

Summary:

Anubis is an anonymous email sender for Unix, BeOS, Win32, and AmigaOS. It supports WinGates, encrypted TLS/SSL connections, remailers, anonymous news posting, and more.

5. MacAnalysis 2.0b

by Lagoon-Software

Relevant URL:

<http://www.securityfocus.com/tools/1989>

Platforms: MacOS, UNIX, Windows 2000, Windows 95/98 and Windows NT

Summary:

MacAnalysis is a security auditing suite for your Macintosh to perform and help implement a security standard for your computer/network by performing a full security check of network protocols, open services, port scans, vulnerable CGI scripts and much more. This will scan your Macintosh, Unix, Windows, and Hardware for any vulnerable security holes!

## VI. SPONSORSHIP INFORMATION

---

This Issue Sponsored by: Foundstone

"Ultimate Hacking: Hands On – NT/2000 Security"

If you're running a Windows network, then this is the intensive 3-day course with everything a hacker knows...that you'll need to know! As a Specialist in Microsoft's Security Services Partner Program, Foundstone knows hacking, security and Microsoft. Register now for the class in New York City, September 25-27 and Irvine, CA December 11-13.

<http://www.foundstone.com/NT>

---

- *Previous message:* [Xno Xutz: "Re: Code Blue"](#)
- *Messages sorted by:* [\[ date \]](#) [\[ thread \]](#) [\[ subject \]](#) [\[ author \]](#) [\[ attachment \]](#)