

# SecurityFocus Microsoft Newsletter #178

**Source:** <http://www.derkeiler.com/Mailing-Lists/securityfocus/focus-ms/2004-03/0005.html>

---

**From:** Marc Fossi ([mfossi\\_at\\_securityfocus.com](mailto:mfossi_at_securityfocus.com))

**Date:** 03/02/04

Date: Mon, 1 Mar 2004 21:05:06 -0700 (MST)

To: Focus-MS <[focus-ms@securityfocus.com](mailto:focus-ms@securityfocus.com)>

SecurityFocus Microsoft Newsletter #178

---

This issue sponsored by: Tenable Security

How do you manage your VULNERABILITIES? Tenable Network Security can help you actively and passively detect them with NeWT and NeVO as well as communicate this information to the people who need to fix them through the Lightning Console. Make recommendations, track remediations, correlate vulnerabilities with IDS events, and create executive reports based on organization, asset type or region. Visit us at:

[http://www.securityfocus.com/sponsor/TenableSecurity\\_ms-secnews\\_040301](http://www.securityfocus.com/sponsor/TenableSecurity_ms-secnews_040301)

---

## I. FRONT AND CENTER

1. Anti-Spam Solutions and Security

## II. MICROSOFT VULNERABILITY SUMMARY

1. Microsoft Windows XP explorer.exe Multiple Memory Corruption...
2. Multiple Outlook/Outlook Express Predictable File Location W...
3. W3C Jigsaw Unspecified Remote URI Parsing Vulnerability
4. Proxy-Pro Professional GateKeeper Web Proxy Buffer Overrun V...
5. Platform Load Sharing Facility EAuth Component Buffer Overfl...
6. Avirt Voice HTTP GET Remote Buffer Overrun Vulnerability
7. Avirt Soho Server HTTP GET Buffer Overrun Vulnerability
8. Avirt Soho Web Service HTTP GET Buffer Overrun Vulnerability
9. Platform Load Sharing Facility EAuth Privilege Escalation Vu...
10. RobotFTP Server Remote Pre-authenticated Command Denial Of S...
11. Apple QuickTime/Darwin Streaming Server DESCRIBE Request Rem...
12. Working Resources BadBlue Server phptest.php Path Disclosure...
13. Microsoft ASN.1 Library Multiple Stack-Based Buffer Overflow...
14. Mozilla Browser Zombie Document Cross-Site Scripting Vulnera...
15. RhinoSoft Serv-U FTP Server MDTM Command Time Argument Buffe...

## III. MICROSOFT FOCUS LIST SUMMARY

1. Preventing OS Detection (Thread)
2. SYN\_SENT to port 8081 (Thread)
3. Log Question (Thread)
4. FPSE Admin Listner on IIS 6.0 (Thread)
5. FW: Preventing OS Detection (Thread)

6. Administrivia: Virus in email (Thread)
7. SecurityFocus Microsoft Newsletter #177 (Thread)
8. Tests to determine ASN.1 patch applicability (Thread)
9. Article Announcement (Thread)

#### IV. NEW PRODUCTS FOR MICROSOFT PLATFORMS

1. Norton Internet Security 2004
2. Dekart Logon
3. AppSentry
4. AppDefend
5. Airscanner Mobile AntiVirus Pro
6. Symantec's Norton Internet Security 2004 Professional

#### V. NEW TOOLS FOR MICROSOFT PLATFORMS

1. Big Sister v0.99b1
2. John the Ripper v1.6.37(dev)
3. GeneSyS v1.0
4. aNTG v2.1
5. Stunnel v4.05
6. Airscanner Mobile AntiVirus Pro v2.5

#### VI. UNSUBSCRIBE INSTRUCTIONS

#### VII. SPONSOR INFORMATION

#### I. FRONT AND CENTER

-----

1. Anti-Spam Solutions and Security  
By Dr. Neal Krawetz

This article is the first of a two-part series that discusses the security issues of spam as well as several current anti-spam methodologies.

<http://www.securityfocus.com/infocus/1762>

#### II. MICROSOFT VULNERABILITY SUMMARY

-----

1. Microsoft Windows XP explorer.exe Multiple Memory Corruption...

BugTraq ID: 9707

Remote: Unknown

Date Published: Feb 20 2004

Relevant URL: <http://www.securityfocus.com/bid/9707>

Summary:

Microsoft Windows Explorer for Windows XP has been reported to be prone to multiple overflow vulnerabilities. The issues exist in the Metafile processing code.

The first issue is reported to occur when a '.emf' (Extended Windows Metafile Format) file with a 'total size' header field set to less than the header size is processed. The header size is used in the vulnerable code to allocate a buffer. Due to insufficient verification of this size, a heap overflow condition can occur if a malformed '.emf' file with a 'total size' field is less than the header size. In order to exploit this issue, an attacker would simply create a '.emf' file sufficient to trigger this issue and place it in any directory. The attacker would then

open the directory via Windows Explorer and view the contents as Thumbnails. Immediate consequences of this attack would result in a denial of service condition. This could also potentially allow for execution of arbitrary code.

The second issue is reported to present itself following the above scenario. It is reported that the rest of the '.emf' file is read until the size/headersize length has been reached and then the file is appended to the header size buffer. This issue could result in an integer overflow condition. Ultimately an attacker may exploit this condition to corrupt sensitive variables in memory to influence execution flow of the affected software into attacker-supplied instructions.

Furthermore, it has been reported that this issue may also affect the image preview window in Windows Explorer resulting in a crash.

If these issues are exploited, it could allow for execution of arbitrary code in the context of the user who invoked the Windows Explorer process.

These vulnerabilities have been tested in Microsoft Windows XP, however, other operating systems provided by Microsoft may be vulnerable as well. Although unconfirmed, these issues may also exist in Microsoft Internet Explorer due to code similarities, possibly making these issues remote in nature.

\*\*Update: There have been reports that indicate that this issue may actually present itself in the shell32.dll library. As a result of this, all applications that are linked to the vulnerable library may also be prone to this vulnerability.

## 2. Multiple Outlook/Outlook Express Predictable File Location W...

BugTraq ID: 9709

Remote: Yes

Date Published: Feb 20 2004

Relevant URL: <http://www.securityfocus.com/bid/9709>

Summary:

Microsoft Outlook and Outlook Express are reported to be prone to store various files which may contain attacker-supplied content in predictable locations, aiding in exploitation of other possible security vulnerabilities.

The following specifics examples of were provided:

Outlook Express stores a temporary copy of embedded sound files in a predictable location (profile\Local Settings\Temp\[filename].[ext]) when these files are opened. The filename and extension in this instance are attacker-specified. An attacker may exploit this weakness in combination with other issues by embedding a malicious HTML file in an e-mail message with an appropriate extension such as .mid or .wav.

Both Outlook and Outlook Express also store temporary copies of HTML documents sent via e-mail in the user's Temp folder using an .html extension. Again, other vulnerabilities may be used to reference the malicious content directly.

Outlook Express is also alleged to store Address Book files in various predictable locations on the client's file system. While the impact of this differs in nature, the Address Book may also be referenced via exploitation of other vulnerabilities, which could disclose sensitive information to remote attacks.

These issues may present a security risk because many known (and potential) Internet Explorer vulnerabilities depend on the attacker being able to directly reference malicious content on a victim system. Given both the ability to place such content on the file system and reference it specifically by location, exploitation of many browser-based vulnerabilities becomes possible. This would often allow for execution of malicious Active Content in the My Computer Zone.

### 3. W3C Jigsaw Unspecified Remote URI Parsing Vulnerability

BugTraq ID: 9711

Remote: Yes

Date Published: Feb 21 2004

Relevant URL: <http://www.securityfocus.com/bid/9711>

Summary:

Jigsaw is an HTTP server produced by W3C. It is implemented in Java, and will run on a wide range of systems, including Microsoft Windows, Linux and other Unix based systems.

Jigsaw is prone to an unspecified remote URI parsing vulnerability. This issue is reportedly due to a failure of the application to properly parse and sanitize user supplied URI input.

The problem revolves around the web server failing to properly handle URI separators.

The results of successful exploitation of this issue are currently unknown, however it is conjectured that this issue may be leveraged to compromise web server readable files outside of the server root directory.

This BID will be updated as further details regarding this issue are disclosed.

### 4. Proxy-Pro Professional GateKeeper Web Proxy Buffer Overrun V...

BugTraq ID: 9716

Remote: Yes

Date Published: Feb 23 2004

Relevant URL: <http://www.securityfocus.com/bid/9716>

Summary:

Professional GateKeeper is a proxy server/firewall application. It is distributed and maintained by Proxy-Pro and available for Microsoft

Windows platforms.

Proxy-Pro Professional GateKeeper is prone to a remotely exploitable buffer overrun that may be triggered by passing HTTP GET requests of excessive length through the web proxy component (which listens on TCP port 3128 by default).

It is possible to cause this condition by submitting an HTTP GET of 4100 bytes or more. Due to insufficient bounds checking of this data, such a request will overrun adjacent regions of memory with attacker-specified data. In this manner, it will be possible for the attacker to overwrite a sensitive variable in memory such as an instruction pointer. This could be exploited to execute arbitrary code in the context of the software.

#### 5. Platform Load Sharing Facility EAuth Component Buffer Overfl...

BugTraq ID: 9719

Remote: Yes

Date Published: Feb 23 2004

Relevant URL: <http://www.securityfocus.com/bid/9719>

Summary:

Load Sharing Facility is a high availability and load balancing software package distributed and maintained by Platform. It is available for Unix, Linux, and Microsoft Windows.

Load Sharing Facility eauth component has been reported prone to a buffer overflow vulnerability. The issue presents itself due to a lack of bounds checks performed on data that is supplied as a value for the '-s' option passed to eauth. By supplying excessive data, an attacker may corrupt data adjacent to the affected buffer and thereby overwrite a saved instruction pointer. An attacker may leverage this issue to influence program execution flow into attacker-supplied instructions. Because the eauth utility is installed setuid root in a default installation this vulnerability may be exploited to gain root privileges.

Additionally it been reported that because eauth is called by daemons, i.e. mbatchd with the '-s' option on attacker supplied data, a remote attacker may exploit this vulnerability from a system that is a part of the affected cluster.

#### 6. Avirt Voice HTTP GET Remote Buffer Overrun Vulnerability

BugTraq ID: 9721

Remote: Yes

Date Published: Feb 23 2004

Relevant URL: <http://www.securityfocus.com/bid/9721>

Summary:

Avirt Voice is an H.323 gateway product for Microsoft Windows operating systems.

Avirt Voice is prone to a remotely exploitable buffer overrun when handling HTTP GET requests of excessive length via the embedded server component listening on TCP port 1080. Due to insufficient bounds checking

of this data, an internal buffer will be overrun, corrupting regions of memory adjacent to the buffer with attacker-specified data. In this manner, it may be possible to corrupt regions of memory and control execution flow of the process, resulting in execution of arbitrary code. The server may also crash when receiving this data.

This issue is reportedly triggered by sending 1113 or more characters in the request.

This issue was reported in Avirt Voice 4.0. Other versions may also be affected.

#### 7. Avirt Soho Server HTTP GET Buffer Overrun Vulnerability

BugTraq ID: 9722

Remote: Yes

Date Published: Feb 23 2004

Relevant URL: <http://www.securityfocus.com/bid/9722>

Summary:

Avirt Soho is an Internet sharing application for Microsoft Windows systems.

Avirt Soho is prone to a remotely exploitable buffer overrun when handling HTTP GET requests of excessive length via the embedded server component listening on TCP port 1080. Due to insufficient bounds checking of this data, an internal buffer will be overrun, corrupting regions of memory adjacent to the buffer with attacker-specified data. In this manner, it may be possible to corrupt regions of memory and control execution flow of the process, resulting in execution of arbitrary code. The server may also crash when receiving this data.

This issue is reportedly triggered by sending 1113 or more characters in the request.

This issue was reported in Avirt Soho 4.3. Other versions may also be affected.

#### 8. Avirt Soho Web Service HTTP GET Buffer Overrun Vulnerability

BugTraq ID: 9723

Remote: Yes

Date Published: Feb 23 2004

Relevant URL: <http://www.securityfocus.com/bid/9723>

Summary:

Avirt Soho is an Internet sharing application for Microsoft Windows systems.

Avirt Soho is prone to a remotely exploitable buffer overrun when handling HTTP GET requests of excessive length via the embedded web service component listening on TCP port 8080. Due to insufficient bounds checking of this data, an internal buffer will be overrun, corrupting regions of memory adjacent to the buffer with attacker-specified data. In this manner, it may be possible to corrupt regions of memory and control

execution flow of the process, resulting in execution of arbitrary code.  
The server may also crash when receiving this data.

This issue is reportedly triggered by sending 2061 or more % characters in the request.

This issue was reported in Avirt Soho 4.3. Other versions may also be affected.

#### 9. Platform Load Sharing Facility EAuth Privilege Escalation Vu...

BugTraq ID: 9724

Remote: Yes

Date Published: Feb 23 2004

Relevant URL: <http://www.securityfocus.com/bid/9724>

Summary:

Load Sharing Facility is a high availability and load balancing software package distributed and maintained by Platform. It is available for Unix, Linux, and Microsoft Windows.

Load Sharing Facility eauth component has been reported prone to a privilege escalation vulnerability. The eauth component is responsible for controlling authentication procedures within Load Sharing Facility. An issue has been reported where an attacker may send commands to Load Sharing Facility as any user. The issue presents itself because eauth uses an environment variable "LSF\_EAUTH\_UID" to determine the UID of the user invoking the binary.

It has been reported that the attacker will require knowledge of "lsfadmin" authentication data prior to the exploitation of this issue. The attacker will exploit this issue by setting LSF\_EAUTH\_UID to the UID of the targeted user, if successful, commands will be executed in Load Sharing Facility as the targeted user.

#### 10. RobotFTP Server Remote Pre-authenticated Command Denial Of S...

BugTraq ID: 9729

Remote: Yes

Date Published: Feb 23 2004

Relevant URL: <http://www.securityfocus.com/bid/9729>

Summary:

RobotFTP Server is an FTP Server for Microsoft Windows operating systems.

RobotFTP server has been reported prone to a denial of service vulnerability. The issue presents itself when certain commands are sent to the service, before authentication is negotiated.

Reportedly when the service handles LIST or CMD directives (or other commands), represented as a hexadecimal string, prior to authentication, the service will fail effectively denying service to legitimate users.

RobotFTP server versions up to and including version 2 are reported prone to this issue.

11. Apple QuickTime/Darwin Streaming Server DESCRIBE Request Rem...

BugTraq ID: 9735

Remote: Yes

Date Published: Feb 24 2004

Relevant URL: <http://www.securityfocus.com/bid/9735>

Summary:

Apple QuickTime/Darwin Streaming Server is server technology which allows you to send streaming QuickTime media to clients across the Internet. It is available for Apple MacOS X, Microsoft Windows and Linux operating systems.

A vulnerability has been identified in Apple QuickTime/Darwin Streaming Server that may allow a remote attacker to cause a denial of service condition in the software. The vulnerability is caused due to improper handling of request data. Specifically, the issue presents itself when the software attempts to parse DESCRIBE requests with specially crafted User-Agent fields. It has been reported that by sending a request containing over 255 characters via the User-Agent field, an attacker may cause an assert error in the 'CommonUtilitiesLib/StringFormatter.h' file leading to a denial of service condition.

Successful exploitation may allow an attacker to cause the affected server to crash, denying service to legitimate users.

QuickTime/Darwin Streaming Server version 4.1.3 is reported to be prone to this issue.

This issue was originally described in Apple Security Update 2004-02-23 Released To Fix Multiple Vulnerabilities (BID 9731).

12. Working Resources BadBlue Server phptest.php Path Disclosure...

BugTraq ID: 9737

Remote: Yes

Date Published: Feb 24 2004

Relevant URL: <http://www.securityfocus.com/bid/9737>

Summary:

BadBlue is a P2P file sharing application distributed by Working Resources. It is available for Microsoft Windows operating systems.

A vulnerability has been reported to exist in the software that may allow an attacker to disclose the installation path. It has been reported that an attacker may disclose the local path of the server by issuing a request for 'phptest.php' script. The path is reportedly included in the source code of the requested page.

Successful exploitation of this vulnerability may allow an attacker to gain sensitive information about the file system that may aid in launching more direct attacks against the system.

BadBlue version 2.4 has been reported to be affected by this issue, however, other versions may be vulnerable as well.

13. Microsoft ASN.1 Library Multiple Stack-Based Buffer Overflow...

BugTraq ID: 9743

Remote: Yes

Date Published: Feb 25 2004

Relevant URL: <http://www.securityfocus.com/bid/9743>

Summary:

Microsoft Windows Abstract Syntax Notation 1 (ASN.1) handling Library (MSASN1.dll) is shipped as a part of the Microsoft Windows Operating System. The MSASN1 library provides an application programmer's interface into Microsoft ASN.1 encoding/decoding and processing functions.

Multiple buffer overflow vulnerabilities have been reported in the Microsoft ASN.1 library. These issues are related to insufficient checking of data supplied via externally supplied length fields in ASN1BERDecDouble and ASN1PERDecDouble functions. Although unconfirmed, these issues could allow an attacker to execute arbitrary code leading to unauthorized access to a vulnerable system.

It has been reported that an attacker may be able to exploit the issue in ASN1BERDecDouble function by passing a value that is larger than 0x10C via 'ASN1BERDecLength' field to the function. Similar issues have been identified in the ASN1PERDecDouble function as well, however, no further details have been disclosed.

These vulnerabilities may have different attack vectors depending upon the services and applications employing the affected functions. Like previously reported issues in the library (BIDs 9633 and 9635), the vulnerable functions could theoretically be used in certificate handling code in Microsoft or third-party software.

Reportedly, the first issue is not exploitable under Windows 2000 SP4 and the second issue has been addressed by the fixes released in MS04-007. This information has not been confirmed by Symantec.

These issues are pending further analysis and will likely be separated into two individual BIDs.

14. Mozilla Browser Zombie Document Cross-Site Scripting Vulnera...

BugTraq ID: 9747

Remote: Yes

Date Published: Feb 25 2004

Relevant URL: <http://www.securityfocus.com/bid/9747>

Summary:

Mozilla is a freely available web browser designed for a number of platforms, including Microsoft Windows and Linux.

Mozilla has been reported to be prone to a cross-site scripting vulnerability. This issue is due to a design error that allows event handlers in a web document from one domain to be executed in the context of another.

This issue is due to the browser allowing a new web page to interact with a previously visited web page before the new page is completely loaded; producing a zombie document. This allows any script events that are activated within a certain time frame to be invoked in the context of the new web page, and thus facilitate cross-site scripting attacks.

The problem surrounds the use of event handlers inside HTML tags. Mozilla does attempt to deactivate these, however they are possible to bypass.

This could permit a remote attacker to create a malicious web page that includes hostile event handling script code. If this page were to redirect to a target page when certain event handling code was activated, the hostile code may be rendered in the web browser of the victim user. This would occur in the security context of the new page and may allow for theft of cookie-based authentication credentials or other attacks.

#### 15. RhinoSoft Serv-U FTP Server MDTM Command Time Argument Buffe...

BugTraq ID: 9751

Remote: Yes

Date Published: Feb 26 2004

Relevant URL: <http://www.securityfocus.com/bid/9751>

Summary:

RhinoSoft Serv-U FTP Server is designed for use with Microsoft Windows operating systems.

Serv-U FTP Server has been reported prone to a remote stack based buffer overflow vulnerability when handling time/date arguments passed to the MDTM FTP command.

The problem exists due to insufficient bounds checking. It has been reported that when a specially crafted MDTM time/date argument is copied into an allocated buffer in Serv-U FTP process memory, data that exceeds the size of the buffer may overrun its bounds and trample adjacent memory. This may allow the attacker to corrupt variables that are saved adjacent to the affected buffer. Ultimately an attacker may leverage this issue to have arbitrary instructions executed in the context of the SYSTEM user.

This vulnerability has been reported to affect Serv-U FTP Server up to but not including version 5.0.0.4.

### III. MICROSOFT FOCUS LIST SUMMARY

---

#### 1. Preventing OS Detection (Thread)

Relevant URL:

<http://www.securityfocus.com/archive/88/355786>

#### 2. SYN\_SENT to port 8081 (Thread)

Relevant URL:

<http://www.securityfocus.com/archive/88/355666>

3. Log Question (Thread)

Relevant URL:

<http://www.securityfocus.com/archive/88/355591>

4. FPSE Admin Listner on IIS 6.0 (Thread)

Relevant URL:

<http://www.securityfocus.com/archive/88/355585>

5. FW: Preventing OS Detection (Thread)

Relevant URL:

<http://www.securityfocus.com/archive/88/355136>

6. Administrivia: Virus in email (Thread)

Relevant URL:

<http://www.securityfocus.com/archive/88/355131>

7. SecurityFocus Microsoft Newsletter #177 (Thread)

Relevant URL:

<http://www.securityfocus.com/archive/88/355115>

8. Tests to determine ASN.1 patch applicability (Thread)

Relevant URL:

<http://www.securityfocus.com/archive/88/355096>

9. Article Announcement (Thread)

Relevant URL:

<http://www.securityfocus.com/archive/88/355028>

#### IV. NEW PRODUCTS FOR MICROSOFT PLATFORMS

---

1. Norton Internet Security 2004

By: Symantec

Platforms: Windows 95/98

Relevant URL: [http://www.symantec.com/sabu/nis/nis\\_pe/](http://www.symantec.com/sabu/nis/nis_pe/)

Summary:

Symantec's Norton Internet Security 2004 provides essential protection from viruses, hackers, and privacy threats. Powerful yet easy to use, this award-winning suite now includes advanced spam-fighting software to filter unwanted mail out of your inbox. Protect yourself, your family, and your PC online with Norton Internet Security 2004.

2. Dekart Logon

By:

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

Relevant URL: [http://www.dekart.com/products/authentication\\_access/logon/](http://www.dekart.com/products/authentication_access/logon/)

Summary:

Dekart Logon is a solution designed to provide an additional level of security for the Microsoft Windows operating system. Access to the Windows environment can only be gained after inserting a USB key or smart card into the appropriate slot and by entering the correct PIN code.

Dekart Logon offers a number of security options: you can select to have Windows access blocked once the key is removed, during a screen saver timeout or other user assigned prompts. This flexibility automatically reduces the possibility of human error by maintaining predefined security levels even if the user leaves their PC unattended.

### 3. AppSentry

By: Integrigy

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

Relevant URL: <http://www.integrigy.com/appsentry.htm>

Summary:

AppSentry is a new generation of security scanner and vulnerability assessment tool. Unlike other security scanners, AppSentry knows the application it is validating ? its technology and data model. The security audits and checks are written specifically for the application being tested. Hackers and mischievous employees often exploit security issues at different layers of the technology stack, thus only a complete and comprehensive security validation will uncover all risks in a multi-tiered environment.

The advantage of AppSentry is now you don't have to separate tools for the operating system, web server, and database. AppSentry is a single tool that can validate and audit the security of the entire application technology stack from operating system to application layer.

AppSentry is available for the following applications –

Oracle E-Business Suite (11i)

Oracle Database (8.x, 8i, 9i, 10g)

Oracle Application Server (9iAS, 10g)

SAP

PeopleSoft

Microsoft SQL Server

### 4. AppDefend

By: Integrigy

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

Relevant URL: <http://www.integrigy.com/appdefend.htm>

Summary:

AppDefend is a new concept in Intrusion Prevention – direct application protection. AppDefend protects the application from attacks and intrusions by blocking attacks before they reach the application.

AppDefend is designed specifically for the application it is protecting. Thus, when implementing for the Oracle E-Business Suite, there is no analysis or other configuration required to provide maximum protection for the application. Integrity has already performed all this work for you – all modules, all versions.

AppDefend is designed to be simple to install and easy to maintain. A straight-forward, yet robust, implementation takes only 15 minutes. No complex configuration or analysis of the application is required.

#### 5. Airscanner Mobile AntiVirus Pro

By: Airscanner Corp.

Platforms: Windows CE

Relevant URL: <http://airscanner.com/downloads/av/av.html>

Summary:

Airscanner Mobile AntiVirus Pro will quarantine or eradicate embedded viruses and malware, has fast, optimized scanning speed based on patent pending technology, has automatic, online updates of virus signatures and scanning engine as well as support for PocketPC 2003/Windows Mobile 2003 and easy online updates.

In addition to an accurate virus scanner, Airscanner Mobile AntiVirus includes these powerful tools for debugging Trojan horses:

- Intercept memory resident viruses with an advanced process discovery tool.
- Debug Trojan hacks with an easy-to-use registry viewer.
- Uncover denial of service attacks with a rapid system analyzer.
- Enter your own custom virus signatures (for experts).
- Perform fast, recursive, and flexibly multithreaded filesystem scanning.

#### 6. Symantec's Norton Internet Security 2004 Professional

By: Symantec

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

Relevant URL: [http://www.symantec.com/smallbiz/nis\\_pr/](http://www.symantec.com/smallbiz/nis_pr/)

Summary:

Symantec's Norton Internet Security 2004 Professional protects you and your business from online threats. It eliminates viruses automatically, blocks hackers, safeguards your personal information, fights spam, increases online productivity, recovers lost or damaged files, and thoroughly deletes confidential data you no longer need. Available in 5 and 10-user Small Office Packs.

#### V. NEW TOOLS FOR MICROSOFT PLATFORMS

---

1. Big Sister v0.99b1

By: Thomas Aeby

Relevant URL: <http://bigsister.sourceforge.net/>

Platforms: Linux, Windows 2000, Windows NT, Windows XP

Summary:

Big Sister is an SNMP-aware monitoring program consisting of a Web-based server and a monitoring agent. It runs under various Unixes and Windows.

2. John the Ripper v1.6.37(dev)

By: Solar Designer

Relevant URL: <http://www.openwall.com/john/>

Platforms: BeOS, DOS, MacOS, Windows 2000, Windows 95/98, Windows NT

Summary:

John the Ripper is a fast password cracker, currently available for many flavors of Unix (11 are officially supported, not counting different architectures), DOS, Win32, BeOS, and OpenVMS. Its primary purpose is to detect weak Unix passwords. It supports several crypt(3) password hash types which are most commonly found on various Unix flavors, as well as Kerberos AFS and Windows NT/2000/XP LM hashes. Several other hash types are added with contributed patches.

3. GeneSyS v1.0

By: Balazs E. Pataki

Relevant URL: <http://genesys.sztaki.hu>

Platforms: UNIX, Windows 2000, Windows NT

Summary:

GeneSyS aims to define and implement a middleware architecture for generic system monitoring and supervision. It is an Information Society Project (IST-2001-34162) sponsored by the European Commission. It provides a middleware- and agent-based approach for system monitoring and management. It uses WebServices technology (SOAP) for communication between components and XML-based descriptions of monitoring information.

4. aNTG v2.1

By: Lucas

Relevant URL: <http://www.thebobo.com/antg.php>

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

Summary:

aNTG (another Network Traffic Grapher) is a PHP program that collects and graphs network traffic statistics on a Linux machine.

5. Stunnel v4.05

By: Michal Trojnara, <Michal.Trojnara@mirt.net>

Relevant URL: <http://stunnel.mirt.net/>

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

Summary:

The stunnel program is designed to work as an SSL encryption wrapper between remote client and local (inetd–startable) or remote server. It can be used to add SSL functionality to commonly used inetd daemons like POP2, POP3, and IMAP servers without any changes in the programs' code. It will negotiate an SSL connection using the OpenSSL or SSLeay libraries. It calls the underlying crypto libraries, so stunnel supports whatever cryptographic algorithms you compiled into your crypto package.

#### 6. Airscanner Mobile AntiVirus Pro v2.5

By: Airscanner Corp

Relevant URL: <http://airscanner.com/downloads/av/av.html>

Platforms: Windows CE

Summary:

Airscanner Corporation is the most trusted name in helping to defend your mobile device from "airborne" computer viruses. From the company that wrote the best–selling technical book Maximum Wireless Security comes a professional strength virus scanner for the Pocket PC.

With the increased wireless connectivity of PDAs and Smartphones comes an increased threat from virus attacks. Save money, time, and data by protecting your valuable Pocket PC now with Airscanner Mobile AntiVirus Pro.

## VI. UNSUBSCRIBE INSTRUCTIONS

---

To unsubscribe send an e–mail message to [ms–secnews–unsubscribe@securityfocus.com](mailto:ms–secnews–unsubscribe@securityfocus.com) from the subscribed address. The contents of the subject or message body do not matter. You will receive a confirmation request message to which you will have to answer.

Alternatively you can also visit <http://www.securityfocus.com/newsletters> and unsubscribe via the website.

If your email address has changed email [listadmin@securityfocus.com](mailto:listadmin@securityfocus.com) and ask to be manually removed.

## VII. SPONSOR INFORMATION

---

This issue sponsored by: Tenable Security

How do you manage your VULNERABILITIES? Tenable Network Security can help you actively and passively detect them with NeWT and NeVO as well as communicate this information to the people who need to fix them through the Lightning Console. Make recommendations, track remediations, correlate vulnerabilities with IDS events, and create executive reports based on organization, asset type or region. Visit us at:

[http://www.securityfocus.com/sponsor/TenableSecurity\\_ms–secnews\\_040301](http://www.securityfocus.com/sponsor/TenableSecurity_ms–secnews_040301)

---

---

Free 30–day trial: firewall with virus/spam protection, URL filtering, VPN,

wireless security

Protect your network against hackers, viruses, spam and other risks with Astaro Security Linux, the comprehensive security solution that combines six applications in one software solution for ease of use and lower total cost of ownership.

Download your free trial at

[http://www.securityfocus.com/sponsor/Astaro\\_focus-ms\\_040301](http://www.securityfocus.com/sponsor/Astaro_focus-ms_040301)

---