

SecurityFocus Microsoft Newsletter #174

Source: <http://www.derkeiler.com/Mailing-Lists/securityfocus/focus-ms/2004-02/0014.html>

From: Marc Fossi (*mfossi_at_securityfocus.com*)

Date: 02/03/04

Date: Tue, 3 Feb 2004 11:18:49 -0700 (MST)

To: Focus-MS <focus-ms@securityfocus.com>

SecurityFocus Microsoft Newsletter #174

This issue sponsored by: Tenable Network Security

Doing network vulnerability scanning? Did you have to ask for permission? Did you have to beg for forgiveness from the admins you caused panic and disruption to? Try NeVO, the worlds only 100% passive vulnerability scanner, from Tenable Network Security!

http://www.securityfocus.com/sponsor/TenableSecurity_ms-secnews_040202

For your 30 day demo please contact: sales@tenablesecurity.com

I. FRONT AND CENTER

1. The Soft Underbelly: Attacking the Client
2. Digital Signatures and European Laws
3. Worms Hit Home
4. We are pleased to announce a new search engine on SecurityFocus.

II. MICROSOFT VULNERABILITY SUMMARY

1. Finjan SurfinGate FHTTP Restart Command Execution Vulnerabil...
2. Novell Netware Enterprise Web Server Multiple Vulnerabilitie...
3. RhinoSoft Serv-U FTP Server MDTM Command Stack Overflow Vuln...
4. Microsoft Windows XP Explorer Self-Executing Folder Vulnerab...
5. mIRC DCC Get Dialog Denial Of Service Vulnerability
6. Cherokee Error Page Cross Site Scripting Vulnerability
7. TCPDump ISAKMP Decoding Routines Denial Of Service Vulnerabi...
8. Microsoft Internet Explorer CLSID File Extension Misrepresen...
9. Internet Security Systems BlackICE PC Protection Upgrade Fil...
10. Internet Security Systems BlackICE PC Protection blackd.exe ...
11. BRS WebWeaver ISAPISkeleton.dll Cross-Site Scripting Vulnera...
12. Loom Software SurfNow Remote HTTP GET Request Denial Of Serv...
13. Macromedia ColdFusion MX Security Sandbox Circumvention Vuln...
14. Kerio Personal Firewall Local Privilege Escalation Vulnerabi...

III. MICROSOFT FOCUS LIST SUMMARY

1. Controlling Admin Access (Thread)
2. SMTP Service in private DMZ OK? (Thread)

3. terminal server (Thread)
4. Encrypt data – SQL Server 2000 (Thread)
5. SecurityFocus Microsoft Newsletter #173 (Thread)

IV. NEW PRODUCTS FOR MICROSOFT PLATFORMS

1. Proactive Windows Security Explorer
2. Outpost Personal Firewall Pro 2.0
3. Dekart Logon
4. AppSentry
5. AppDefend
6. Airscanner Mobile AntiVirus Pro

V. NEW TOOLS FOR MICROSOFT PLATFORMS

1. MUTE File Sharing v0.2.2
2. Airscanner Mobile AntiVirus Pro v1.4
3. WinRelay v2.0
4. GNU Generic Security Service Library v0.0.10
5. OSIRIS v3.0.0
6. mrtg v2.10.13

VI. UNSUBSCRIBE INSTRUCTIONS

VII. SPONSOR INFORMATION

I. FRONT AND CENTER

1. The Soft Underbelly: Attacking the Client
By Tom Vogt

This article discusses the lack of security inside many corporate networks once hackers have breached the border perimeter and firewall. Client-based attack vectors, malicious payloads and their potential impact to an organization are also discussed.

<http://www.securityfocus.com/infocus/1758>

2. Digital Signatures and European Laws
By Mirella Mazzeo

This article discusses the security requirements for electronic communications and commerce with European governments and many European-based businesses. It will also give an overview of the current trends for public key infrastructure in Europe, useful for any organization that does business with the EU.

<http://www.securityfocus.com/infocus/1756>

3. Worms Hit Home
By Kelly Martin

The fact that each of us can only control and manage the patches and virus definitions on machines within our own borders means little as we watch the promulgation of malcode on millions of home machines outside of our control.

<http://www.securityfocus.com/columnists/216>

4. We are pleased to announce a new search engine on SecurityFocus, offering faster and more intuitive results. Features include site wide or section specific searching by author, headline or entire document and sorting by date, headline or URL.

II. MICROSOFT VULNERABILITY SUMMARY

1. Finjan SurfinGate FHTTP Restart Command Execution Vulnerabil...

BugTraq ID: 9478

Remote: Yes

Date Published: Jan 23 2004

Relevant URL: <http://www.securityfocus.com/bid/9478>

Summary:

SurfinGate is a commercially available content filtering and application firewall package. It is distributed by Finjan, and available for the Sun Solaris and Microsoft Windows platforms.

Finjan SurfinGate is prone to a vulnerability that may permit remote attackers to execute certain management commands (using the FHTTP protocol) through the management control port (3141/TCP). The source of the vulnerability is insufficient authorization of remotely supplied restart commands. While it may be possible to filter access by untrusted IPs to the control port, these commands could also be issued via the HTTP proxy included in the software, so will appear to originate from the localhost in this instance and could theoretically bypass access controls for untrusted external IPs.

It has been reported that commands could be issued to restart the server, most likely resulting in a denial of service.

2. Novell Netware Enterprise Web Server Multiple Vulnerabilitie...

BugTraq ID: 9479

Remote: Yes

Date Published: Jan 23 2004

Relevant URL: <http://www.securityfocus.com/bid/9479>

Summary:

Multiple vulnerabilities have been identified in Novell Netware Enterprise Web Server that may allow an attacker to carry out cross-site scripting attacks, disclose sensitive information, and load potentially malicious files on a vulnerable server.

It has been reported that the software may be prone to multiple cross-site scripting vulnerabilities that may allow a remote attacker to launch cross-site scripting attacks. Reportedly, the software contains various variables that are prone to these attacks due to insufficient sanitization of user-supplied data. Various proof of concepts including vulnerable variables have been provided in the report. Successful exploitation of these issues may allow an attacker to steal cookie based authentication credentials and carry out other attacks.

An information disclosure issue has been identified in the software as well. It has been reported that a remote attacker may be able to view sensitive data such as internal IP addresses and other unspecified server information. This attack may be carried out by accessing certain files such as snoop.jsp, SnoopServlet, env.bas, and lcgitest.nlm. Successful exploitation of this issue may allow an attacker to gain access to sensitive data that could be used to launch further attacks against a system.

Another issue may allow an attacker to access directory listings on a vulnerable server. It has been reported that this issue may be exploited by accessing various pages on a vulnerable server. Successful exploitation of this issue may allow an attacker to gain access to sensitive data that could be used to launch further attacks against a system. A path disclosure issue may also exist in the software that may allow an attacker to gain sensitive information about the file system that could aid in launching more direct attacks against the system. This issue may be exploited via a malicious URI request including '\ ' characters.

Finally, it has been reported that an attacker may be able to load Microsoft Hypertext Template (.htt) files to a server. This issue may allow an attack to upload potentially malicious files to the server that may corrupt other files.

These issues are reported to affect Netware Enterprise Web Server 5.1 and 6.0. Other versions may be affected as well.

These issues are currently undergoing further analysis. This cumulative BID will be separated into individual entries when analysis is complete.

3. RhinoSoft Serv-U FTP Server MDTM Command Stack Overflow Vuln...

BugTraq ID: 9483

Remote: Yes

Date Published: Jan 24 2004

Relevant URL: <http://www.securityfocus.com/bid/9483>

Summary:

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

Serv-U FTP Server is reportedly prone to a stack-based buffer overflow.

When a 'site chmod' command is issued specifying a non-existent file, the FTP server will call the following sprintf command to display an error message:

```
sprintf(dst, "%s: No such file or directory.", filename);
```

The problem exists due to insufficient bounds checking on the 'dst' variable. The buffer assigned to this variable is 256 bytes. If the non-existent filename specified is greater than 256 bytes, the buffer will be overrun, resulting in a failure of the FTP server. It has been conjectured that this vulnerability may be exploited to execute arbitrary

code in the security context of the Serv-U FTP Server process.

It is important to note that this issue could only be exploited on a writeable directory on the FTP server.

This vulnerability was reported to affect all versions of Serv-U FTP Server prior to 4.2.

4. Microsoft Windows XP Explorer Self-Executing Folder Vulnerab...

BugTraq ID: 9487

Remote: Yes

Date Published: Jan 26 2004

Relevant URL: <http://www.securityfocus.com/bid/9487>

Summary:

A vulnerability has been reported in Microsoft Windows XP that may result in execution of malicious code in the context of the currently logged in user. The flaw exists in Windows Explorer and may allow for executable content that is referenced from inside of a folder to be executed automatically when the folder is accessed. It has been demonstrated that an HTML folder that includes malicious scripting can call an arbitrary executable, which could be self-contained in the folder.

It should be noted that the folder must exist on the vulnerable system, though it is possible that remote attackers could entice users to open a malicious folder via e-mail or by hosting it on a website. For example, a remote attacker could include the malicious folder in an archive, which a user may then download and then open. In this case, exploitation would occur when the folder inside the archive is accessed by the victim user.

This vulnerability poses a security risk since it is assumed that opening a folder is a safe action and that executable content cannot be run when a folder is accessed. A locally based attacker could use this issue to gain elevated privileges on a system by placing the malicious folder in a location that will expectedly be accessed by another user. Remote attackers who can entice a user to download and access the malicious folder could exploit this issue to gain unauthorized remote access to a vulnerable system in the context of the victim user. Additionally, it has been reported that this issue may be exploitable remotely if the malicious folder is accessed from an SMB share.

5. mIRC DCC Get Dialog Denial Of Service Vulnerability

BugTraq ID: 9492

Remote: Yes

Date Published: Jan 26 2004

Relevant URL: <http://www.securityfocus.com/bid/9492>

Summary:

mIRC is a chat client for the IRC protocol, designed for Microsoft Windows based operating systems.

A vulnerability has been reported to exist in mIRC that may allow a remote attacker to crash a vulnerable mIRC client. The condition is most likely

present due to insufficient boundary checking performed on 'DCC GET' requests.

It has been reported that the issue will present itself only in certain circumstances. Specifically, the victim must have a minimized "DCC GET" dialog; this dialog must then be opened to "GET" a file that is named with a filename of excessive length. This will reportedly cause a violation in the affected software resulting in a crash.

Although unconfirmed, due to the nature of this vulnerability it has been conjectured that a remote attacker may potentially lever this issue to have arbitrary code executed in the context of the affected mIRC client.

It should be noted that although mIRC version 6.12 has been reported to be prone to this issue, other versions might be affected as well.

6. Cherokee Error Page Cross Site Scripting Vulnerability

BugTraq ID: 9496

Remote: Yes

Date Published: Jan 26 2004

Relevant URL: <http://www.securityfocus.com/bid/9496>

Summary:

Cherokee is a web server distributed under the GNU public license. It is available for numerous platforms, including Microsoft Windows and Unix/Linux variants.

Cherokee has been reported to contain a cross-site scripting vulnerability. This issue is due to the server failing to check and filter user-supplied strings issued to the server in a web request, which are then included directly in error output.

An attacker can exploit this issue by crafting a URI link containing the malevolent HTML or script code, and enticing a user to follow it. If this link were followed, the hostile code may be rendered in the web browser of the victim user. This would occur in the security context of the affected web server and may allow for theft of cookie-based authentication credentials or other attacks.

7. TCPDump ISAKMP Decoding Routines Denial Of Service Vulnerabi...

BugTraq ID: 9507

Remote: Yes

Date Published: Jan 27 2004

Relevant URL: <http://www.securityfocus.com/bid/9507>

Summary:

tcpdump is a freely available, open source network monitoring tool. It is available for the Unix, Linux, and Microsoft Windows operating systems.

A vulnerability has been identified in the software that may allow a remote attacker to cause a denial of service condition in the software. The issue occurs due to the way tcpdump decodes Internet Security Association and Key Management Protocol (ISAKMP) packets. A remote

attacker may cause the software to enter an infinite loop by sending malformed ISAKMP packets resulting in a crash or hang.

Although unconfirmed, due to the nature of this issue, an attacker may leverage the issue by exploiting an unbounded memory copy operation to overwrite the saved return address/base pointer, causing an affected procedure to return to an address of their choice. Successful exploitation of this issue may allow an attacker to execute arbitrary code with the privileges of the tcpdump process in order to gain unauthorized access.

tcpdump versions prior to 3.8.1 have been reported to be prone to this issue.

8. Microsoft Internet Explorer CLSID File Extension Misrepresenten...

BugTraq ID: 9510

Remote: Yes

Date Published: Jan 27 2004

Relevant URL: <http://www.securityfocus.com/bid/9510>

Summary:

A vulnerability has been reported in Microsoft Internet Explorer that may allow files to be misrepresented to client users.

The following proof-of-concept example was released which specifies the CLSID for HTML applications as a file extension and includes an additional file name and extension after the CLSID:

```
malware.{3050f4d8-98B5-11CF-BB82-00AA00BDCE0B}fun_ball_gites_pie_throw%2Empeg
```

The browser appears to present the content to the user as the file name and type specified after the CLSID, when the actual content type is determined by the CLSID (which specifies an HTML application). It is not known at this time where the security flaw lies but it has been demonstrated that such a filename may be used to misrepresent the file type. The dot to separate the additional file extension may need to be URL-encoded (%2E) for exploitation to be successful, though this has not been confirmed.

This issue could be exploited to disguise executable content in the form of an HTML application (HTA) file as a file type that may appear innocuous to a victim user. The file will appear to be of an attacker-specified type in the file download dialog presented to the user. The user may then download/open that file under the assumption it is safe, which could result in execution of malicious code on the client system in the context of the victim user. It should also be noted that the file name may be prepended by '...' in the download dialog, to abbreviate the malicious file name and CLSID extension in the prefix.

This issue could be exploited via a malicious web page or possibly through e-mail.

This issue was reported in Internet Explorer 6.0. Earlier versions of the browser may also be affected.

9. Internet Security Systems BlackICE PC Protection Upgrade Fil...

BugTraq ID: 9513

Remote: No

Date Published: Jan 28 2004

Relevant URL: <http://www.securityfocus.com/bid/9513>

Summary:

Internet Security Systems BlackICE PC Protection is a firewall/IDS implementation for desktop systems running Microsoft Windows.

BlackICE PC Protection is reported to install various .ini files with insecure permissions after an upgrade. This may allow non-administrative users to modify or replace these files, facilitating other attacks. This could affect various security properties as configuration information for the software may be altered by an unauthorized user. There is also a buffer overrun that exists in the software when parsing various directives included in .ini files, as described in BID 9514. This additional issue could be exploited once the permissions have been lowered.

The following files are reported to have lowered permissions after an upgrade:

blackice.ini

firewall.ini

protect.ini

sigs.ini

It should be noted that exploitation of other latent vulnerabilities, such as those described in BID 8577 could create a situation where a remote attacker could place a hostile .ini on the local file system that is designed to weaken the security provided by the software or exploit the buffer overrun described in BID 9514. It has also been reported that the Application Protection feature, if enabled, will prevent various files associated with the software from unauthorized modification.

This issue has been reported to occur when the software is upgraded to version 3.6.cbz. It is not known if other upgrades present the same security risk.

10. Internet Security Systems BlackICE PC Protection blackd.exe ...

BugTraq ID: 9514

Remote: No

Date Published: Jan 28 2004

Relevant URL: <http://www.securityfocus.com/bid/9514>

Summary:

Internet Security Systems BlackICE PC Protection is a firewall/IDS implementation for desktop systems running Microsoft Windows.

It is reported that BlackICE PC Protection is prone to a locally exploitable buffer overrun when handling excessive input in certain

configuration directives for various .ini files included with the software. While these files are allegedly not writeable by non-administrative users in the default install, it has been reported that they may be globally writeable by all system users after a software upgrade (as described in BID 9513).

The issue is reportedly exposed when a 'packetLog.fileprefix=' directive of 217+ bytes in length is included in the blackice.ini file. This will allow the attacker to influence the contents of various system registers such as EIP and ECX, effectively permitting the attacker to control execution flow of the blackd.exe process.

Given the ability of a local attacker to modify the contents of these files, it will be possible to execute arbitrary with SYSTEM privileges since the blackd.exe process runs in SYSTEM context.

This issue could also be exploited remotely if an attacker can exploit other vulnerabilities to cause a malicious version of a .ini file to be placed on the local system. This might occur through exploitation of latent vulnerabilities in Internet Explorer, such as those described in BID 8577.

11. BRS WebWeaver ISAPISkeleton.dll Cross-Site Scripting Vulnera...

BugTraq ID: 9516

Remote: Yes

Date Published: Jan 28 2004

Relevant URL: <http://www.securityfocus.com/bid/9516>

Summary:

BRS WebWeaver is an HTTP/FTP server implementation for Microsoft Windows platforms.

BRS WebWeaver has been reported prone to a cross-site scripting vulnerability. The issue is known to exist in the ISAPISkeleton.dll script. Arguments supplied to this script in web requests will be output in dynamically generated web pages without adequate sanitization of HTML and script code. As a result, an attacker may create a malicious link to the vulnerable server that includes embedded HTML and script code. If this link is followed by a victim user, hostile code embedded in the link may be rendered in the user's browser in the context of the server.

Successful exploitation could permit theft of cookie-based authentication credentials. The attacker could also theoretically influence how server pages will be rendered to the victim user, allowing for other attacks.

This issue could affect various web applications hosted on the server, since these web applications could be in the same domain as the server and therefore hostile script code may be able to access properties of these applications.

This issue was reported in BRS WebWeaver 1.07. Earlier versions may also be affected.

12. Loom Software SurfNow Remote HTTP GET Request Denial Of Serv...

BugTraq ID: 9519

Remote: Yes

Date Published: Jan 28 2004

Relevant URL: <http://www.securityfocus.com/bid/9519>

Summary:

SurfNOW is a commercially-available proxy software package designed to obscure identity and protect privacy on the Internet. It is available for the Microsoft Windows platform.

A problem has been identified in the handling of specific types of requests by SurfNOW. Upon receiving specially crafted requests, it is possible for a remote attacker to crash a vulnerable implementation, denying service to the user.

The problem is in the handling of excessive data in HTTP header fields. An attacker with access to the proxy server can potentially submit a request of excessive length, causing the server to become unstable. It has been reported that this can reliably produce a crash in the proxy server after multiple such requests are submitted. The attacker must reportedly send HTTP GET requests that are 490k in length to reproduce this issue.

This issue may be indicative of a boundary condition error. This information, however, is conjecture based on reports by the researcher. If this information does prove to be true, it may likely be possible to exploit this condition to execute code with the privileges of the proxy server process.

13. Macromedia ColdFusion MX Security Sandbox Circumvention Vuln...

BugTraq ID: 9521

Remote: No

Date Published: Jan 28 2004

Relevant URL: <http://www.securityfocus.com/bid/9521>

Summary:

ColdFusion MX is the application server for developing and hosting infrastructure distributed by Macromedia. It is available as a standalone product for Unix, Linux, and Microsoft Operating Systems.

ColdFusion MX has been reported prone to a security sandbox circumvention vulnerability. The issue is reported to exist because programmers have the ability to create instances of classes without using "CreateObject()" or "<cfobject>" tags. It has been reported that the security sandbox does not prevent this behavior.

This issue cannot be exploited remotely, but the vulnerability may present a danger in a shared hosted environment.

An attacker may exploit this issue to circumvent the security sandbox of ColdFusion MX.

This issue has been reported to affect ColdFusion MX 6.1.

14. Kerio Personal Firewall Local Privilege Escalation Vulnerabi...

BugTraq ID: 9525

Remote: No

Date Published: Jan 29 2004

Relevant URL: <http://www.securityfocus.com/bid/9525>

Summary:

Kerio Personal Firewall (KPF) is a desktop firewall solution that performs stateful packet inspection. It is available for the Microsoft Windows platform.

A vulnerability has been reported to be present in the software that may allow a local attacker to gain elevated privileges. The problem occurs due to a function used to load configuration files. It has been reported that this function can be exploited to execute malicious applications with SYSTEM privileges.

Successful exploitation of this issue may allow an attacker to execute malicious applications with SYSTEM privileges on a vulnerable system that may lead to full compromise.

Kerio Personal Firewall 2.1.5 has been reported to be prone to this issue, however, other versions could be affected as well.

III. MICROSOFT FOCUS LIST SUMMARY

1. Controlling Admin Access (Thread)

Relevant URL:

<http://www.securityfocus.com/archive/88/352161>

2. SMTP Service in private DMZ OK? (Thread)

Relevant URL:

<http://www.securityfocus.com/archive/88/352158>

3. terminal server (Thread)

Relevant URL:

<http://www.securityfocus.com/archive/88/352041>

4. Encrypt data – SQL Server 2000 (Thread)

Relevant URL:

<http://www.securityfocus.com/archive/88/351981>

5. SecurityFocus Microsoft Newsletter #173 (Thread)

Relevant URL:

<http://www.securityfocus.com/archive/88/351305>

IV. NEW PRODUCTS FOR MICROSOFT PLATFORMS

1. Proactive Windows Security Explorer

By: Elcomsoft Co. Ltd.

Platforms: Windows 2000, Windows NT, Windows XP

Relevant URL: <http://www.elcomsoft.com/pwsex.html#>

Summary:

Proactive Windows Security Explorer (PWSEX) is a password security test tool that's designed to allow Windows NT, Windows 2000, and Windows XP-based systems administrators to identify and close security holes in their networks. Proactive Windows Security Explorer helps secure networks by executing an audit of account passwords, and exposing insecure account passwords. If it is possible to recover the password within a reasonable time, the password is considered insecure.

An administrator can also use it to recover any lost password and access a user's Windows account. Proactive Windows Security Explorer works by analyzing user password hashes and recovering plain-text passwords.

2. Outpost Personal Firewall Pro 2.0

By: Agnitum

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

Relevant URL: <http://www.outpost.uk.com>

Summary:

New Outpost Personal Firewall Pro 2.0 outdistances the award-winning Outpost Personal Firewall Pro 1.0 on multiple levels, from enhanced privacy features to ease-of-use. As the foremost security application for personal computers, Outpost Personal Firewall Pro 2.0 gives you the latest in personal firewall technology, making version 2.0 the clear security choice for your system.

3. Dekart Logon

By:

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

Relevant URL: 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.

4. AppSentry

By: Integrigy

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

Relevant URL: <http://www.integrigy.com/appentry.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

5. 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. Integrigy 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.

6. 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.

V. NEW TOOLS FOR MICROSOFT PLATFORMS

1. MUTE File Sharing v0.2.2

By: Jason Rohrer

Relevant URL: <http://mute-net.sourceforge.net/>

Platforms: Linux, MacOS, Os Independent, Windows 2000, Windows 95/98

Summary:

MUTE File Sharing is an anonymous, decentralized search-and-download file sharing system. Several people have described MUTE as the "third generation file sharing network" (From Napster to Gnutella to MUTE, with each generation getting less centralized and more anonymous). MUTE uses algorithms inspired by ant behavior to route all messages, include file transfers, through a mesh network of neighbor connections.

2. Airscanner Mobile AntiVirus Pro v1.4

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.

3. WinRelay v2.0

By: Arne Vidstrom <arne.vidstrom@ntsecurity.nu>

Relevant URL: <http://www.ntsecurity.nu/toolbox/winrelay/>

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

Summary:

WinRelay is a TCP/UDP forwarder/redirector. You can choose the port and IP it will listen on, the source port and IP that it will connect from, and the port and IP that it will connect to.

4. GNU Generic Security Service Library v0.0.10

By: Simon Josefsson

Relevant URL: <http://www.gnu.org/software/gss/>

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

Summary:

Generic Security Service (GSS) is an implementation of the Generic Security Service API (GSSAPI). It is used by network applications to provide security services, such as authenticating SMTP/IMAP, via the GSSAPI SASL mechanism. It consists of a library and a manual, and a Kerberos 5 mechanism that supports mutual authentication and the DES and 3DES ciphers.

5. OSIRIS v3.0.0

By: The Shmoo Group

Relevant URL: <http://osiris.shmoo.com>

Platforms: BSDI, FreeBSD, Linux, MacOS, OpenBSD, UNIX, Windows 2000, Windows NT, Windows XP

Summary:

Osiris is a host integrity management system that can be used to monitor changes to a network of hosts over time and report those changes back to the administrator(s). Currently, this includes monitoring any changes to the filesystems. Osiris takes periodic snapshots of the filesystem and stores them in a database. These databases, as well as the configurations and logs, are all stored on a central management host. When changes are detected, Osiris will log these events to the system log and optionally send email to an administrator. In addition to files, Osiris has preliminary support for the monitoring of other system information including user lists, file system details, kernel modules, and network interface configurations (not included with in this beta release).

6. mrtg v2.10.13

By: Tobias Oetiker

Relevant URL: <http://people.ee.ethz.ch/~oetiker/webtools/mrtg/>

Platforms: POSIX, Windows 2000, Windows NT

Summary:

The Multi Router Traffic Grapher (MRTG) is a tool to monitor the traffic load on network-links. MRTG generates HTML pages containing GIF/PNG images

which provide a live visual representation of this traffic.

VI. UNSUBSCRIBE INSTRUCTIONS

To unsubscribe send an e-mail message to 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 and ask to be manually removed.

VII. SPONSOR INFORMATION

This issue sponsored by: Tenable Network Security

Doing network vulnerability scanning? Did you have to ask for permission? Did you have to beg for forgiveness from the admins you caused panic and disruption to? Try NeVO, the worlds only 100% passive vulnerability scanner, from Tenable Network Security!

http://www.securityfocus.com/sponsor/TenableSecurity_ms-secnews_040202

For your 30 day demo please contact: sales@tenablesecurity.com
