

SecurityFocus Microsoft Newsletter #182

Source: <http://www.derkeiler.com/Mailing-Lists/securityfocus/focus-ms/2004-03/0044.html>

From: Marc Fossi (*mfossi_at_securityfocus.com*)

Date: 03/30/04

Date: Tue, 30 Mar 2004 07:13:55 -0700 (MST)

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

SecurityFocus Microsoft Newsletter #182

This Issue is Sponsored by: Check Point

Introducing the world's first and only complete Internal Security Gateway:
Check Point InterSpect.

Built specifically to protect internal networks, Check Point InterSpect provides intelligent worm defense, network zone segmentation, quarantine capabilities, and LAN protocol protection – all in one easy to deploy appliance that protects your network from threats within.

Learn more about Check Point InterSpect at:

http://www.securityfocus.com/sponsor/CheckPoint_sf-news_040315

I. FRONT AND CENTER

1. Security Patches by Modem? Forget it!
2. When Gaming is a Gamble

II. MICROSOFT VULNERABILITY SUMMARY

1. NullSoft Winamp Long File Name Denial of Service Vulnerability
2. NullSoft Winamp Malformed File Name Denial of Service Vulnerability
3. Microsoft Windows XP Explorer.EXE Remote Denial of Service Vulnerability
4. Samba SMBPrint Sample Script Insecure Temporary File Handling Vulnerability
5. Apache Error Log Escape Sequence Injection Vulnerability
6. Expinion.net Member Management System ID Parameter SQL Injection Vulnerability
7. Expinion.net Member Management System Multiple Cross-Site Scripting Vulnerabilities
8. Expinion.net News Manager Lite Multiple Vulnerabilities
9. phpBB profile.php avatarselect Cross-Site Scripting Vulnerability
10. Joel Palmius Mod_Survey Survey Input Field HTML Injection Vulnerability
11. phpBB Multiple Input Validation Vulnerabilities
12. Invision Gallery Multiple SQL Injection Vulnerabilities
13. Centrinity FirstClass HTTP Server TargetName Parameter Cross-Site Scripting Vulnerability
14. ReGet Software ReGet Directory Traversal Vulnerability
15. Ipswitch WS_FTP Multiple Vulnerabilities
16. Foxmail Remote Buffer Overflow Vulnerability
17. Hiyte HiGuest Message Field HTML Injection Vulnerability

18. DameWare Mini Remote Control Server Weak Random Key Generati...
19. DameWare Mini Remote Control Server Clear Text Encryption Ke...
20. Microsoft Visual C++ MFC ISAPI Extension Denial Of Service V...
21. Kerio WinRoute Firewall Unspecified Malformed HTTP Header De...
22. Virtual Programming VP-ASP Shopping Cart CatalogID SQL Injec...
23. PicoPhone Internet Phone Remote Buffer Overflow Vulnerabilit...
24. NexGen FTP Server Remote Directory Traversal Vulnerability
25. HP Web Jetadmin Printer Firmware Update Script Arbitrary Fil...
26. HP Web Jetadmin setinfo.hts Script Directory Traversal Vulne...
27. HP Web Jetadmin Remote Arbitrary Command Execution Vulnerabi...
28. ESignal Remote Buffer Overflow Vulnerability
29. Nival Interactive Etherlords Remote Denial Of Service Vulner...

III. MICROSOFT FOCUS LIST SUMMARY

1. process tracking (Thread)
2. Hardening TCP/IP Stack; conflicting sources (Thread)
3. security tools (Thread)

IV. NEW PRODUCTS FOR MICROSOFT PLATFORMS

1. Norton Internet Security 2004
2. East-Tec Eraser 2004
3. Steganos Security Suite 6
4. Airscanner Mobile AntiVirus Pro
5. Symantec's Norton Internet Security 2004 Professional
6. secure2trust

V. NEW TOOLS FOR MICROSOFT PLATFORMS

1. Securepoint Firewall and VPN Server v4.0 (S4)
2. Telconi Terminal for Cisco IOS v0.5a
3. Cryptonit v0.9.3
4. CryptoHeaven v2.3.2
5. TrustSight Security Hardening Tool v 1.0 Beta
6. Big Sister v0.99b1

VI. UNSUBSCRIBE INSTRUCTIONS

VII. SPONSOR INFORMATION

I. FRONT AND CENTER

1. Security Patches by Modem? Forget it!
By Scott Granneman

Let's face it – there is no way for dial-up users on any major operating system to keep their computers up-to-date and patched. OK, maybe "no way" is an exaggeration. How about, "a difficult, burdensome, time-consuming, very prone to failure way?"

<http://www.securityfocus.com/columnists/230>

2. When Gaming is a Gamble
By Mark Rasch

A new Justice Department policy threatens to jail security professionals who help lock down online gambling sites anywhere in the world.

<http://www.securityfocus.com/columnists/229>

II. MICROSOFT VULNERABILITY SUMMARY

1. NullSoft Winamp Long File Name Denial of Service Vulnerabili...

BugTraq ID: 9920

Remote: Yes

Date Published: Mar 19 2004

Relevant URL: <http://www.securityfocus.com/bid/9920>

Summary:

It has been reported that Winamp may be prone to a denial of service vulnerability when processing files with a name exceeding 246 characters. Immediate consequences of this issue may result in the application crashing. Although unconfirmed, due to the nature of this vulnerability an attack could result in a buffer overflow condition and may lead to arbitrary code execution. Any code execution would occur in the context of the user running the application.

Winamp 5.02 was identified as the vulnerable version, however, it is possible that other versions are affected as well.

Conflicting reports have surfaced regarding this issue. It is possible that this issue may not be valid. This BID will be updated or retired as more information becomes available.

2. NullSoft Winamp Malformed File Name Denial of Service Vulner...

BugTraq ID: 9923

Remote: Yes

Date Published: Mar 19 2004

Relevant URL: <http://www.securityfocus.com/bid/9923>

Summary:

It has been reported that Winamp may be prone to a denial of service vulnerability when processing malformed file names. This issue is reported to present itself when a file with a malformed file name is processed by the application. Specifically, if the file name contains an excessive amount of characters and has '.mid' extension.

Winamp 5.01 an prior were reported to be prone to this issue, however, it is possible that other versions are affected as well.

3. Microsoft Windows XP Explorer.EXE Remote Denial of Service V...

BugTraq ID: 9924

Remote: Yes

Date Published: Mar 19 2004

Relevant URL: <http://www.securityfocus.com/bid/9924>

Summary:

Microsoft Windows Explorer for Windows XP has been reported to be prone to a remote denial of service vulnerability.

This issue is due to a failure of the application to properly validate user-supplied input via the 'shell:' command. The 'shell:' command is a

parameter that a user can specify when including a URI in an HTML tag. This command allows the HTML script to potentially execute any program specified after the 'shell:' command.

Successful exploitation of this issue would cause the affected application to crash, denying service to legitimate users.

4. Samba SMBPrint Sample Script Insecure Temporary File Handlin...

BugTraq ID: 9926

Remote: No

Date Published: Mar 19 2004

Relevant URL: <http://www.securityfocus.com/bid/9926>

Summary:

It has been reported that the 'smbprint-new.sh' sample Samba script is prone to a local insecure temporary file handling symbolic link vulnerability. This issue is due to a design error that allows the application to insecurely write to a temporary file that is created with a predictable file name.

An attacker may exploit this issue to corrupt arbitrary files. This corruption may potentially result in the elevation of privileges, or in a system wide denial of service.

It should be noted that the 'smbprint-new.sh' is a sample script located in the 'examples' directory. This script is not intended for commercial use. The 'smbprint' script included in the 'packaging' directory is not vulnerable to this issue. Individual package distributions may vary.

5. Apache Error Log Escape Sequence Injection Vulnerability

BugTraq ID: 9930

Remote: Yes

Date Published: Mar 20 2004

Relevant URL: <http://www.securityfocus.com/bid/9930>

Summary:

It has been reported that the Apache web server is prone to a remote error log escape sequence injection vulnerability. This issue is due to an input validation error that may allow escape character sequences to be injected into apache log files.

This may facilitate exploitation of issues such as those found in BIDs 6936 and 6938.

This issue may allow an attacker to carry out a number of actions including arbitrary file creation and code execution on the affected system.

6. Expinion.net Member Management System ID Parameter SQL Injec...

BugTraq ID: 9931

Remote: Yes

Date Published: Mar 20 2004

Relevant URL: <http://www.securityfocus.com/bid/9931>

Summary:

It has been reported that Member Management System may be prone to a SQL injection vulnerability that may allow a remote attacker to inject malicious SQL syntax into database queries. The problem is reported to exist in the 'ID' parameter contained within the 'resend.asp' and 'news_view.asp' scripts.

Member Management System version 2.1 has been reported to be affected by this issue, however, other versions may be vulnerable as well.

7. Expinion.net Member Management System Multiple Cross-Site Sc...

BugTraq ID: 9932

Remote: Yes

Date Published: Mar 20 2004

Relevant URL: <http://www.securityfocus.com/bid/9932>

Summary:

It has been reported that a number of Member Management System scripts are prone to cross-site scripting vulnerabilities. These issues are reportedly due to a failure to sanitize user input and so allow HTML and script code that may facilitate cross-site scripting attacks. The issues are reported to affect the 'err' parameter of 'error.asp' script and the 'register.asp' script.

Member Management System version 2.1 has been reported to be affected by this issue, however, other versions may be vulnerable as well.

8. Expinion.net News Manager Lite Multiple Vulnerabilities

BugTraq ID: 9935

Remote: Yes

Date Published: Mar 20 2004

Relevant URL: <http://www.securityfocus.com/bid/9935>

Summary:

Multiple vulnerabilities have been identified in the application that may allow an attacker to carry out SQL injection, cross-site scripting, and account hijacking attacks.

The issues exist in the 'comment_add.asp', 'search.asp', 'category_news_headline.asp', 'more.asp', 'category_news.asp', and 'ews_sort.asp' scripts. Further more a cookie account hijacking issue was also discovered in the application that may allow a remote attacker to gain administrative access to application's administrative interface.

News Manager Lite 2.5 is reported to be affected by these issues, however, other versions may be affected as well.

9. phpBB profile.php avatarselect Cross-Site Scripting Vulnerab...

BugTraq ID: 9938

Remote: Yes

Date Published: Mar 22 2004

Relevant URL: <http://www.securityfocus.com/bid/9938>

Summary:

It has been reported that phpBB may be prone to a cross-site scripting vulnerability that may allow an attacker to execute arbitrary HTML or script code in a user's browser. The issue exists due to insufficient sanitization of user-supplied input via the 'avatarselect' form parameter of 'profile.php' script.

phpBB 2.0.6d has been reported to be prone to this issue, however, other versions could be affected as well.

10. Joel Palmius Mod_Survey Survey Input Field HTML Injection Vu...

BugTraq ID: 9941

Remote: Yes

Date Published: Mar 22 2004

Relevant URL: <http://www.securityfocus.com/bid/9941>

Summary:

Mod_Survey is prone to HTML injection attacks via survey input fields. They may permit remote attackers to persistently inject HTML and script code into surveys, which may be rendered in the web browser of administrative or other users.

Exploitation could permit for theft of cookie-based authentication credentials. Other attacks are also possible.

11. phpBB Multiple Input Validation Vulnerabilities

BugTraq ID: 9942

Remote: Yes

Date Published: Mar 22 2004

Relevant URL: <http://www.securityfocus.com/bid/9942>

Summary:

It has been reported that phpBB may be prone to multiple vulnerabilities that could allow an attacker to carry out SQL injection and cross-site scripting attacks. These vulnerabilities result from insufficient sanitization of user-supplied input via the 'id' parameter of 'admin_smilies.php' module and the 'style_id' parameter of 'admin_styles' module.

phpBB versions 2.0.7a and prior are reported to be prone to these issues.

12. Invision Gallery Multiple SQL Injection Vulnerabilities

BugTraq ID: 9944

Remote: Yes

Date Published: Mar 22 2004

Relevant URL: <http://www.securityfocus.com/bid/9944>

Summary:

It has been reported that Invision Gallery may be prone to multiple sql injection vulnerabilities, allowing an attacker to influence SQL query logic. The issues exist due to insufficient sanitization of user-supplied data via the 'img', 'cat', 'sort_key', 'order_key', 'user' and 'album' parameters of the gallery module accessed via the 'index.php' script.

Invision Gallery is a gallery system that can be used as a plugin for Invision Power Board. Invision Gallery 1.0.1 is reported to be prone to these issues, however, other versions could be affected as well.

13. Centrinity FirstClass HTTP Server TargetName Parameter Cross...

BugTraq ID: 9950

Remote: Yes

Date Published: Mar 22 2004

Relevant URL: <http://www.securityfocus.com/bid/9950>

Summary:

It has been reported that FirstClass HTTP Server may be prone to a cross-site scripting vulnerability that may allow a remote attacker to execute arbitrary HTML or script code in a user's browser. The issue presents itself due to insufficient sanitization of user-supplied data via the 'TargetName' parameter of 'Upload.shtml' script.

Since this vulnerability affects the web server there is a possibility of an attacker crossing domains if multiple domains are hosted on one web server. The vendor has reported that this vulnerability only affects the 'standard' template set. The 'webmail' and 'mobile' template sets do not contain the 'Upload.shtml' script.

Centrinity FirstClass versions 7.1 and prior may be vulnerable to this issue.

14. ReGet Software ReGet Directory Traversal Vulnerability

BugTraq ID: 9951

Remote: Yes

Date Published: Mar 22 2004

Relevant URL: <http://www.securityfocus.com/bid/9951>

Summary:

It has been reported that ReGet may be prone to a directory traversal vulnerability that may allow remote attackers to upload files to arbitrary locations on a target system. The attacker may supply encoded directory traversal sequences in the URI parameter so that the requested file is saved outside of the default download directory specified by the user.

ReGet Deluxe 3.0 build 121 has been reported to be prone to this issue, however, other versions could be affected as well.

15. Ipswitch WS_FTP Multiple Vulnerabilities

BugTraq ID: 9953

Remote: Yes

Date Published: Mar 23 2004

Relevant URL: <http://www.securityfocus.com/bid/9953>

Summary:

Multiple vulnerabilities have been identified in the WS_FTP Server and client applications. These vulnerabilities may allow remote attackers to execute arbitrary code, cause denial of service attacks and gain administrative level access to a server.

The issues include two remote buffer overflow vulnerabilities in the client, a denial of service vulnerability in the server and an access validation issue in the server leading to remote command execution with SYSTEM privileges.

These issues are undergoing further analysis. This BID will be divided into separate issues as analysis is completed.

16. Foxmail Remote Buffer Overflow Vulnerability

BugTraq ID: 9954

Remote: Yes

Date Published: Mar 23 2004

Relevant URL: <http://www.securityfocus.com/bid/9954>

Summary:

It has been reported that Foxmail is prone to a remote buffer overflow vulnerability. This issue is due to a failure of the application to verify buffer boundaries when processing user supplied email headers.

A remote attacker may potentially exploit this issue to cause the email client to crash, denying service to the victim user. It is also possible to further leverage this issue in order to execute arbitrary code; this code would be executed in the security context of the user running the affected email client.

17. Hiyte HiGuest Message Field HTML Injection Vulnerability

BugTraq ID: 9955

Remote: Yes

Date Published: Mar 23 2004

Relevant URL: <http://www.securityfocus.com/bid/9955>

Summary:

Hiyte's HiGuest guestbook software is prone to HTML injection attacks. This issue is exposed via the message form field in the guestbook entry submission form.

Exploitation could permit remote attackers to persistently inject hostile HTML and script code into guestbook content. This could allow for theft of cookie-based authentications or other attacks, such as those which misrepresent guestbook content.

18. DameWare Mini Remote Control Server Weak Random Key Generati...

BugTraq ID: 9957

Remote: Yes

Date Published: Mar 23 2004

Relevant URL: <http://www.securityfocus.com/bid/9957>

Summary:

It has been reported that DameWare Mini Remote Control Server may prone to a weak random key generation weakness that could allow an attacker to determine the key and therefore ultimately expose encrypted authentication credentials. This issue exists due to a weak random bit generator is being used to generate encryption keys. These keys are used by the application to encrypt user credentials.

Dameware Mini Remote Control version 4.1.0.0 is reported to be affected by this issue, however, it is possible that prior versions are vulnerable as well.

19. DameWare Mini Remote Control Server Clear Text Encryption Ke...

BugTraq ID: 9959

Remote: Yes

Date Published: Mar 23 2004

Relevant URL: <http://www.securityfocus.com/bid/9959>

Summary:

It has been reported that DameWare Mini Remote Control Server may be prone to a clear text encryption key disclosure vulnerability. The issue presents itself because the file encryption key is sent over the network in plain text format.

Dameware Mini Remote Control version 4.1.0.0 is reported to be affected by this issue, however, it is possible that prior versions are vulnerable as well.

20. Microsoft Visual C++ MFC ISAPI Extension Denial Of Service V...

BugTraq ID: 9963

Remote: Yes

Date Published: Mar 24 2004

Relevant URL: <http://www.securityfocus.com/bid/9963>

Summary:

It has been reported that ISAPI (Internet Server Application Programming Interface) extensions that are built using the MFC (Microsoft Foundation Classes) static library in Microsoft Visual C++ are prone to a denial of service vulnerability. This could occur during POST requests when the ISAPI extension is under heavy load.

Microsoft Visual C++ is included in Microsoft Visual Studio. This reportedly affects Microsoft Visual C++/Studio 6.

21. Kerio WinRoute Firewall Unspecified Malformed HTTP Header De...

BugTraq ID: 9964

Remote: Yes

Date Published: Mar 24 2004

Relevant URL: <http://www.securityfocus.com/bid/9964>

Summary:

It has been reported that WinRoute Firewall may be prone to an unspecified remote denial of service vulnerability that may allow an attacker to cause the firewall process to crash or hang. This issue occurs when the application parses malformed HTTP headers.

WinRoute Firewall versions 5.1.9 and prior are reported prone to this issue.

Due to a lack of details, further information is not available at the moment. This BID will be updated as more information becomes available.

22. Virtual Programming VP-ASP Shopping Cart CatalogID SQL Injec...

BugTraq ID: 9967

Remote: Yes

Date Published: Mar 24 2004

Relevant URL: <http://www.securityfocus.com/bid/9967>

Summary:

It has been reported that the VP-ASP Shopping Cart is prone to a remote SQL injection vulnerability. This issue is due to a failure of the application to properly sanitize user input before using it in an SQL query.

It may be possible for an attacker to leverage this issue to disclose the administrator password hash, or other sensitive information contained within the database by exploiting this issue.

23. PicoPhone Internet Phone Remote Buffer Overflow Vulnerabilit...

BugTraq ID: 9969

Remote: Yes

Date Published: Mar 24 2004

Relevant URL: <http://www.securityfocus.com/bid/9969>

Summary:

It has been reported that Picophone is prone to a remote buffer overflow vulnerability. This issue is due to the application failing to verify the size of user input before storing it in a finite buffer.

Successful exploitation of this issue will cause a denial of service condition to be triggered. The attacker may also leverage this issue to execute arbitrary code; this code would be executed in the security context of the user running the affected process.

24. NexGen FTP Server Remote Directory Traversal Vulnerability

BugTraq ID: 9970

Remote: Yes

Date Published: Mar 24 2004

Relevant URL: <http://www.securityfocus.com/bid/9970>

Summary:

It has been reported that the Nexgen FTP server is prone to a remote directory traversal vulnerability. This issue is due to a failure of the application to properly sanitize file request strings from authenticated users.

Successful exploitation of this vulnerability may allow a remote attacker to gain access to sensitive information that may be used to launch further attacks against a vulnerable system.

25. HP Web Jetadmin Printer Firmware Update Script Arbitrary Fil...

BugTraq ID: 9971

Remote: Yes

Date Published: Mar 24 2004

Relevant URL: <http://www.securityfocus.com/bid/9971>

Summary:

HP Web Jetadmin is prone to an issue which may permit remote users to upload arbitrary files to the management server.

This issue exists in the printer firmware update script. Given the ability to place arbitrary files on the server to an attacker-specified location, it may be possible to execute arbitrary code, though this will require exploitation of other known vulnerabilities, such as BID 9972 "HP Web Jetadmin setinfo.hts Script Directory Traversal Vulnerability".

Authentication, if it has been enabled, would be required to exploit this issue.

This issue was reported in HP Web Jetadmin version 7.5.2546 on a Windows platform. Other versions may be similarly affected.

26. HP Web Jetadmin setinfo.hts Script Directory Traversal Vulne...

BugTraq ID: 9972

Remote: Yes

Date Published: Mar 24 2004

Relevant URL: <http://www.securityfocus.com/bid/9972>

Summary:

It has been reported that HP Web JetAdmin may be prone to a directory traversal vulnerability allowing remote attackers to access information outside the server root directory. The problem exists due to insufficient sanitization of user-supplied data passed via the 'setinclude' parameter of 'setinfo.hts' script.

This vulnerability can be combined with HP Web Jetadmin Firmware Update Script Arbitrary File Upload Weakness (BID 9971) to upload malicious files to a vulnerable server in order to gain unauthorized access to a host.

This issue has been tested with an authenticated account on HP Web Jetadmin version 7.5.2546 running on a Windows platform.

27. HP Web Jetadmin Remote Arbitrary Command Execution Vulnerabi...

BugTraq ID: 9973

Remote: Yes

Date Published: Mar 24 2004

Relevant URL: <http://www.securityfocus.com/bid/9973>

Summary:

Reportedly HP web Jetadmin is prone to a remote arbitrary command execution vulnerability. This issue is due to a failure of the application to properly validate and sanitize user supplied input.

Successful exploitation of this issue will allow a malicious user to execute arbitrary commands on the affected system.

This issue has been tested with an authenticated account on HP Web Jetadmin version 7.5.2546 running on a Windows platform.

28. ESignal Remote Buffer Overflow Vulnerability

BugTraq ID: 9978

Remote: Yes

Date Published: Mar 25 2004

Relevant URL: <http://www.securityfocus.com/bid/9978>

Summary:

It has been reported that eSignal is prone to a remote buffer overflow vulnerability. This issue is due to the application failing to verify the size of user input before storing it in a finite buffer.

This issue may be leveraged by an attacker to modify process memory. This may cause a denial of service condition in the process as a result of the memory manipulation. The attacker may further leverage this issue in order to execute arbitrary code; this code would be executed in the security context of the user running the affected process.

This issue is reported to affect versions 7.5 and 7.6 of the software. It is quite likely however that earlier versions are affected as well.

29. Nival Interactive Etherlords Remote Denial Of Service Vulner...

BugTraq ID: 9979

Remote: Yes

Date Published: Mar 25 2004

Relevant URL: <http://www.securityfocus.com/bid/9979>

Summary:

A remote denial of service vulnerability has been reported in Etherlords and Etherlords II. This issue is due to a failure of the application to properly validate user-supplied network data.

By issuing a packet containing a large value specifying the size of the data block to follow, a malicious user can leverage this issue by causing the client or server to crash.

III. MICROSOFT FOCUS LIST SUMMARY

1. process tracking (Thread)

Relevant URL:

<http://www.securityfocus.com/archive/88/358849>

2. Hardening TCP/IP Stack; conflicting sources (Thread)

Relevant URL:

<http://www.securityfocus.com/archive/88/358227>

3. security tools (Thread)

Relevant URL:

<http://www.securityfocus.com/archive/88/358131>

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/

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. East-Tec Eraser 2004

By: EAST Technologies

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

Relevant URL: <http://www.east-tec.com/eraser/index.htm>

Summary:

East-Tec Eraser ("Eraser" in short) is an advanced security application for Windows 95/98/Me/NT/2000/XP designed to help you completely eliminate sensitive data from your computer and protect your computer and Internet privacy.

Eraser introduces a new meaning for the verb TO ERASE. Erasing a file now means wiping its contents beyond recovery, scrambling its name and dates and finally removing it from disk. When you want to get rid of sensitive files or folders beyond recovery, add them to the Eraser list of doomed files and ask Eraser to do the job. Eraser offers tight integration with the Windows shell, so you can drag files and folders from Explorer and drop them in Eraser, or you can erase them directly from Explorer by selecting Erase beyond recovery from the context menu.

3. Steganos Security Suite 6

By: Steganos

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

Relevant URL: <http://www.steganos.com/?product=SSS6&language=en>

Summary:

With Steganos Data Safe, Internet Trace Destructor 6.5, Password Manager, steganography function, E-Mail-Encryption, Deep Cleaning Shredder and much more, The Steganos Security Suite has been one of the best-selling encryption products for years and is used by 2 million people worldwide. Only the most modern encryption algorithms, such as the Advanced Encryption Standard (AES) are used. You can now save up to 128 GB* to its four virtual drives in real time – enough space for your film archive, large graphics files and other sensitive data.

4. 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.

5. 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/

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.

6. secure2trust

By: Avoco Secure

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

Relevant URL: http://www.avocosecure.com/html_pages/products_service.html

Summary:

secure2trust gives you the power to create documents that remain under your corporate control throughout their entire existence. Even if you allow another party to have a copy of your original document you can be sure that the copy will always have your original controls as part of its properties. The digital rights options which will control printing, copying, viewing, etc give you persistent and secure digital asset protection and intellectual property control. Digital rights mechanisms are the only way to ensure document integrity in a persistent way for both inter and intra company communications.

V. NEW TOOLS FOR MICROSOFT PLATFORMS

1. Securepoint Firewall and VPN Server v4.0 (S4)

By: Lutz Hausmann

Relevant URL: <http://www.securepoint.cc/>

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

Summary:

Securepoint Firewall and VPN Server is a high-performance application designed to offer full protection for network assets. The Security Manager offers a graphical user interface with many features, different configurations, and advanced reporting functions. The Securepoint server is a complete firewall and VPN software system with an operating system based on a secure Linux. VPN operation supports PPTP and IPsec (X.509 certificates, preshared, RSA signature). You can use the firewall on a standard PC with 2 to 16 network cards (including Ethernet, ADSL, ISDN). It is very easy to install and administer. The Securepoint Security Manager is available in English, German, and Spanish, and works in online and offline mode.

2. Telconi Terminal for Cisco IOS v0.5a

By: Stywiz

Relevant URL: <http://www.telconi.com/>

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

Summary:

Telconi Terminal is a unique network management application with interactive full-screen configuration editing, browsing, help facility support, debugging, and more. It focuses on common Cisco IOS functionality present with any hardware or software configuration, and complements the command line interface with a rich set of features. It is intended for users with knowledge of Cisco IOS, and is designed to work with any IOS-based device, such as routers and switches.

3. Cryptonit v0.9.3

By: IDEALX <idx-pki@idealx.org>

Relevant URL: <http://cryptonit.org/>

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

Summary:

Cryptonit is a client side cryptographic tool which allows you to encrypt/decrypt and sign/verify files with PKI (Public Key Infrastructure) certificates.

4. CryptoHeaven v2.3.2

By: Marcin Kurzawa <marcin@cryptoheaven.com>

Relevant URL: <http://www.cryptoheaven.com/>

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

Summary:

CryptoHeaven offers secure email and online file sharing/storage. Its main features are secure and highly encrypted services such as group collaboration, file sharing, email, online storage, and instant messaging.

It integrates multi-user based security into email, instant messaging, and file storage and sharing in one unique package. It provides real time communication for text and data transfers in a multi-user secure environment. The security and usability of CryptoHeaven is well-balanced; even the no-so-technically oriented computer users can enjoy this crypto product with very high level of encryption.

5. TrustSight Security Hardening Tool v 1.0 Beta

By: Syhunt Inf. Ltd.

Relevant URL: http://www.syhunt.com/section.php?id=sec_hardening

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

Summary:

TrustSight Security Hardening Tool parses the web server's configuration files to detect security configuration errors. Examines the web server's security configuration with close to 50 security checks. Supports Apache and PHP configuration files. Produces simple, easy to read reports.

6. 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.

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 is Sponsored by: Check Point

Introducing the world's first and only complete Internal Security Gateway: Check Point InterSpect.

Built specifically to protect internal networks, Check Point InterSpect provides intelligent worm defense, network zone segmentation, quarantine capabilities, and LAN protocol protection – all in one easy to deploy appliance that protects your network from threats within.

Learn more about Check Point InterSpect at:

http://www.securityfocus.com/sponsor/CheckPoint_sf-news_040315

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
