

SecurityFocus Microsoft Newsletter #212

Source: <http://www.derkeiler.com/Mailing-Lists/securityfocus/focus-ms/2004-10/0097.html>

From: Marc Fossi (*mfossi_at_securityfocus.com*)

Date: 10/28/04

Date: Thu, 28 Oct 2004 08:33:06 -0600 (MDT)

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

SecurityFocus Microsoft Newsletter #212

This Issue is Sponsored By: SecurityFocus

Stay up to date. All the latest news, columns, jobs and more in a convenient html newsletter – Even a glimpse of upcoming columns and feature articles! Sign up today!

<http://www.securityfocus.com/htmlnewsletter/subscribe>

I. FRONT AND CENTER

1. Issues Discovering Compromised Machines
2. The Latest Tool in Competition: Hacking

II. MICROSOFT VULNERABILITY SUMMARY

1. ARJ Software UNARJ Remote Directory Traversal Vulnerability
2. CoolPHP Multiple Remote Input Validation Vulnerabilities
3. Microsoft Outlook 2003 Security Policy Bypass Vulnerability
4. Microsoft Outlook Express Plaintext Email Security Policy By...
5. Best Software SalesLogix Multiple Remote Vulnerabilities
6. IBM Lotus Domino Cross-Site Scripting and HTML Injection Vul...
7. Cabextract Remote Directory Traversal Vulnerability
8. Microsoft Internet Explorer Valid File Drag and Drop Embedde...
9. Microsoft Internet Explorer HTML Help Control Local Zone Sec...
10. Maxthon Web Browser Cross-Domain Dialog Box Spoofing Vulnera...
11. Avant Browser Cross-Domain Dialog Box Spoofing Vulnerability
12. Mozilla Browser Cross-Domain Tab Window Form Field Focus Vul...
13. Opera Web Browser Cross-Domain Dialog Box Spoofing Vulnerabi...
14. Maxthon Web Browser Cross-Domain Tab Window Form Field Focus...
15. Avant Browser Cross-Domain Tab Window Form Field Focus Vulne...
16. Akella Privateer's Bounty: Age of Sail II Remote Buffer Over...
17. Gaim MSN SLP Remote Buffer Overflow Vulnerability
18. Gaim MSN Remote File Transfer Denial Of Service Vulnerabilit...
19. Gaim MSN Remote SLP Denial Of Service Vulnerability
20. Zinf/Freeamp Unspecified Insecure Temporary File Creation Vu...
21. Microsoft Windows XP WAV File Handler Denial Of Service Vuln...

22. LibTIFF OJPEG Heap Buffer Overflow Vulnerability
23. Code-Crafters Ability Server FTP STOR Argument Remote Buffer...

III. MICROSOFT FOCUS LIST SUMMARY

NO NEW POSTS FOR THE WEEK 2004-10-19 to 2004-10-26.

IV. NEW PRODUCTS FOR MICROSOFT PLATFORMS

1. Firewall RuleMaker
2. CAT Cellular Authentication Token and eAuthentication Servic...
3. KeyCaptor Keylogger
4. SpyBuster
5. FreezeX
6. NeoExec for Active Directory

V. NEW TOOLS FOR MICROSOFT PLATFORMS

1. antinat v0.81
2. PopMessenger 1.60
3. ByteShelter I 1.0
4. DiskInternals Uneraser 2.01
5. DiskInternals NTFS Reader 1.01
6. Airscanner Mobile Firewall 1.0

VI. UNSUBSCRIBE INSTRUCTIONS

VII. SPONSOR INFORMATION

I. FRONT AND CENTER

1. Issues Discovering Compromised Machines By Anton Chuvakin

This article discusses the discovery of compromised machines in large enterprise environments, and offers some suggestions on correlating NIDS and HIPS logs to avoid false positives.

<http://www.securityfocus.com/infocus/1808>

2. The Latest Tool in Competition: Hacking By Mark Rasch

A new federal case illustrates the role computer intrusion is taking in the high-stakes world of niche Internet commerce.

<http://www.securityfocus.com/columnists/273>

II. MICROSOFT VULNERABILITY SUMMARY

1. ARJ Software UNARJ Remote Directory Traversal Vulnerability BugTraq ID: 11436

Remote: Yes

Date Published: Oct 16 2004

Relevant URL: <http://www.securityfocus.com/bid/11436>

Summary:

Reportedly ARJ Software UNARJ is affected by a remote directory traversal vulnerability. This issue is due to a failure of the application to properly sanitize or validate file names prior to compression or decompression.

SecurityFocus Microsoft: SecurityFocus Microsoft Newsletter #212

This issue may allow an attacker to arbitrarily overwrite files with a user's privileges when a malicious compressed file is decompressed with the affected application.

2. CoolPHP Multiple Remote Input Validation Vulnerabilities

BugTraq ID: 11437

Remote: Yes

Date Published: Oct 16 2004

Relevant URL: <http://www.securityfocus.com/bid/11437>

Summary:

Reportedly CoolPHP is affected by multiple remote input validation vulnerabilities. These issues are due to a failure of the application to properly sanitize user supplied input prior to using it to make critical actions.

An attacker can leverage these issues to steal cookie-based authentication credentials as well as carry out other malicious activities through cross-site scripting attacks. An attacker can also leverage this issue to execute arbitrary server-side scripts using file include attacks.

3. Microsoft Outlook 2003 Security Policy Bypass Vulnerability

BugTraq ID: 11446

Remote: Yes

Date Published: Oct 18 2004

Relevant URL: <http://www.securityfocus.com/bid/11446>

Summary:

Microsoft Outlook 2003 is reported prone to a security policy bypass vulnerability.

It is reported that by including a base64 encoded image in an email and labeling that image in a sufficient manner, it is then possible to reference this base64 encoded image.

This will result in a policy bypass because the image will be automatically rendered when the email is viewed in Outlook 2003. Although this issue is reported to affect Outlook 2003, other mail transfer agents may also be affected.

4. Microsoft Outlook Express Plaintext Email Security Policy By...

BugTraq ID: 11447

Remote: Yes

Date Published: Oct 18 2004

Relevant URL: <http://www.securityfocus.com/bid/11447>

Summary:

Microsoft Outlook Express is reported prone to a security policy bypass vulnerability.

The vulnerability presents itself if an attached image file is referenced using a specially crafted CID URI.

This will result in a policy bypass because the image will be automatically rendered when the email is viewed in Outlook Express.

5. Best Software SalesLogix Multiple Remote Vulnerabilities

BugTraq ID: 11450

Remote: Yes

Date Published: Oct 18 2004

Relevant URL: <http://www.securityfocus.com/bid/11450>

Summary:

Best Software SalesLogix is affected by multiple vulnerabilities. These issues are due to design errors that

reveal sensitive information, access control validation issues that allow unauthorized access and input validation issues facilitating SQL injection attacks.

An attacker may leverage these issues to manipulate and disclose database contents through SQL injection attacks, steal authentication credentials due to information disclosure vulnerabilities and bypass authentication to gain administrator access to the server.

6. IBM Lotus Domino Cross-Site Scripting and HTML Injection Vul...

BugTraq ID: 11458

Remote: Yes

Date Published: Oct 18 2004

Relevant URL: <http://www.securityfocus.com/bid/11458>

Summary:

It is reported that Lotus Domino is susceptible to a cross-site scripting and an HTML injection vulnerability. These issues are due to a failure of the application to properly sanitize user-supplied input.

The cross-site scripting issue could permit a remote attacker to create a malicious URI link that includes hostile HTML and script code. If this link were to be 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 site and may allow for theft of cookie-based authentication credentials or other attacks.

The HTML injection issue may allow an attacker to inject malicious HTML and script code into the application. An unsuspecting user viewing a page that contains the malicious comment will have the attacker-supplied script code executed within their browser in the context of the vulnerable site. This issue may be leveraged to steal cookie based authentication credentials. Other attacks are also possible.

7. Cabextract Remote Directory Traversal Vulnerability

BugTraq ID: 11460

Remote: Yes

Date Published: Oct 19 2004

Relevant URL: <http://www.securityfocus.com/bid/11460>

Summary:

cabextract is reported prone to a remote directory traversal vulnerability. This issue presents itself due to insufficient sanitization of user-supplied data.

An attacker may exploit this issue to corrupt or manipulate sensitive data. This may aid in further attacks against a computer.

cabextract versions 1.0 and prior are reported prone to this issue.

8. Microsoft Internet Explorer Valid File Drag and Drop Embedde...

BugTraq ID: 11466

Remote: Yes

Date Published: Oct 20 2004

Relevant URL: <http://www.securityfocus.com/bid/11466>

Summary:

The Microsoft cumulative Internet Explorer patch (MS04-038) attempted to limit what files may be dragged and dropped onto the local computer from the Internet Zone to prevent executable objects from being placed on the file system in this manner. However, a number of file types are still permitted for drag and drop operations. It has demonstrated that it is possible to embed hostile HTML and script code in one of these file types, remove the file extension and then allow the operating system to dynamically determine the file

type based on its contents.

If this issue were combined with other vulnerabilities, such as that described in BID 11467, it may result in execution of arbitrary code on the client computer.

9. Microsoft Internet Explorer HTML Help Control Local Zone Sec...

BugTraq ID: 11467

Remote: Yes

Date Published: Oct 20 2004

Relevant URL: <http://www.securityfocus.com/bid/11467>

Summary:

Microsoft Windows XP SP2 and Internet Explorer 6 SP2 have included enhanced Local Zone security restrictions to prevent various exploits that have depended on the previous relaxed security settings associated with this Security Zone. A proof-of-concept has been released demonstrating that it is possible to bypass these restrictions through the use of the 'hhctrl.ocx' HTML ActiveX control.

If the attacker is able to place malicious HTML/scripting content on the system through another vulnerability, such as BID 11466, then this control could be exploited to bypass Local Zone security restrictions that would normally prevent the content from being executed. The proof-of-concept also employs various ADODB methods such as ADODB.Connection and ADODB.recordset to write malicious arbitrary code to the file system, in the form of an .HTA file.

10. Maxthon Web Browser Cross-Domain Dialog Box Spoofing Vulnera...

BugTraq ID: 11470

Remote: Yes

Date Published: Oct 20 2004

Relevant URL: <http://www.securityfocus.com/bid/11470>

Summary:

Maxthon web browser is reported prone to a cross-domain dialog box spoofing vulnerability. This issue may allow a remote attacker to carry out phishing style attacks as an attacker may exploit this vulnerability to spoof the interface of a trusted web site.

11. Avant Browser Cross-Domain Dialog Box Spoofing Vulnerability

BugTraq ID: 11472

Remote: Yes

Date Published: Oct 20 2004

Relevant URL: <http://www.securityfocus.com/bid/11472>

Summary:

Avant Browser is reported prone to a cross-domain dialog box spoofing vulnerability. This issue may allow a remote attacker to carry out phishing style attacks as an attacker may exploit this vulnerability to spoof an interface of a trusted web site.

12. Mozilla Browser Cross-Domain Tab Window Form Field Focus Vul...

BugTraq ID: 11474

Remote: Yes

Date Published: Oct 20 2004

Relevant URL: <http://www.securityfocus.com/bid/11474>

Summary:

A cross-domain tab window form field focus vulnerability reportedly affects Mozilla browser and all browsers derived from it. This issue is due to an access validation error that allows a web page to gain access to form fields in other web pages rendered in different tabs of the same browser window.

SecurityFocus Microsoft: SecurityFocus Microsoft Newsletter #212

This issue may be leveraged to facilitate convincing phishing style attacks designed to reveal sensitive information such as passwords and financial details.

13. Opera Web Browser Cross–Domain Dialog Box Spoofing Vulnerabi...

BugTraq ID: 11475

Remote: Yes

Date Published: Oct 20 2004

Relevant URL: <http://www.securityfocus.com/bid/11475>

Summary:

Opera is reported prone to a cross–domain dialog box spoofing vulnerability. This issue may allow a remote attacker to carry out phishing style attacks as an attacker may exploit this vulnerability to spoof an interface of a trusted web site.

Opera version 7.54 is reported susceptible to this issue, but other versions may also be affected.

14. Maxthon Web Browser Cross–Domain Tab Window Form Field Focus...

BugTraq ID: 11476

Remote: Yes

Date Published: Oct 20 2004

Relevant URL: <http://www.securityfocus.com/bid/11476>

Summary:

A cross–domain tab window form field focus vulnerability reportedly affects the Maxthon Web browser. This issue is due to an access validation error that allows a web page to gain access to form fields in other web pages rendered in different tabs of the same browser window.

This issue may be leveraged to facilitate convincing phishing style attacks designed to reveal sensitive information such as passwords and financial details.

15. Avant Browser Cross–Domain Tab Window Form Field Focus Vulne...

BugTraq ID: 11478

Remote: Yes

Date Published: Oct 20 2004

Relevant URL: <http://www.securityfocus.com/bid/11478>

Summary:

A cross–domain tab window form field focus vulnerability reportedly affects Avant Browser. This issue is due to an access validation error that allows a web page to gain access to form fields in other web pages rendered in different tabs of the same browser window.

This issue may be leveraged to facilitate convincing phishing style attacks designed to reveal sensitive information such as passwords and financial details.

16. Akella Privateer's Bounty: Age of Sail II Remote Buffer Over...

BugTraq ID: 11479

Remote: Yes

Date Published: Oct 20 2004

Relevant URL: <http://www.securityfocus.com/bid/11479>

Summary:

Akella Privateer's Bounty: Age of Sail II is reportedly affected by a remote buffer overflow vulnerability. This issue is due to a failure of the application to do sufficient bounds checking on user–supplied input.

SecurityFocus Microsoft: SecurityFocus Microsoft Newsletter #212

An attacker can leverage this issue to execute arbitrary code on an affected computer with the privileges of a user running a vulnerable version of the game.

17. Gaim MSN SLP Remote Buffer Overflow Vulnerability

BugTraq ID: 11482

Remote: Yes

Date Published: Oct 20 2004

Relevant URL: <http://www.securityfocus.com/bid/11482>

Summary:

Gaim is reportedly affected by a remote buffer overflow vulnerability in its MSN SLP message functionality of gaim. This issue is due to a failure of the application to verify buffer bounds when copying user-supplied input.

An attacker can leverage this issue to execute arbitrary code on an affected computer with the privileges of the user that executed the vulnerable application.

18. Gaim MSN Remote File Transfer Denial Of Service Vulnerabilit...

BugTraq ID: 11483

Remote: Yes

Date Published: Oct 20 2004

Relevant URL: <http://www.securityfocus.com/bid/11483>

Summary:

Gaim is affected by a remote MSN file transfer denial of service vulnerability. This issue is due to a failure of the application to properly handle exceptional conditions.

An attacker may leverage this issue to cause an affected client to crash, denying service to legitimate users.

19. Gaim MSN Remote SLP Denial Of Service Vulnerability

BugTraq ID: 11484

Remote: Yes

Date Published: Oct 20 2004

Relevant URL: <http://www.securityfocus.com/bid/11484>

Summary:

Gaim is affected by a remote MSN SLP denial of service vulnerability. This issue is due to a failure of the application to properly handle exceptional conditions.

An attacker may leverage this issue to cause an affected client to crash, denying service to legitimate users.

20. Zinf/Freeamp Unspecified Insecure Temporary File Creation Vu...

BugTraq ID: 11490

Remote: No

Date Published: Oct 21 2004

Relevant URL: <http://www.securityfocus.com/bid/11490>

Summary:

Zinf/Freeamp are affected by an unspecified insecure temporary file creation vulnerability. This issue is likely due to a design error that causes the application to fail to verify the existence of a file before writing to it.

An attacker may leverage this issue to overwrite arbitrary files with the privileges of an unsuspecting user that activates the vulnerable application.

21. Microsoft Windows XP WAV File Handler Denial Of Service Vuln...

BugTraq ID: 11503

Remote: Yes

Date Published: Oct 22 2004

Relevant URL: <http://www.securityfocus.com/bid/11503>

Summary:

Microsoft Windows XP is reported prone to a denial of service vulnerability. The issue exists due to a lack of sufficient sanitization performed on WAV file header values before they are processed.

If an exploit attempt is successful, the Windows Explorer process will begin to consume CPU resources. An attacker may exploit this vulnerability to deny service to legitimate users.

22. LibTIFF OJPEG Heap Buffer Overflow Vulnerability

BugTraq ID: 11506

Remote: Yes

Date Published: Oct 22 2004

Relevant URL: <http://www.securityfocus.com/bid/11506>

Summary:

LibTIFF is affected by a heap buffer overflow vulnerability. This issue is due to a failure of the application to properly perform boundary checks prior to copying user-supplied strings into finite process buffers.

An attacker may leverage this issue to execute arbitrary code on a vulnerable computer with the privileges of the user running the vulnerable application, facilitating unauthorized access. This issue may also be leveraged to cause an affected application to crash.

23. Code-Crafters Ability Server FTP STOR Argument Remote Buffer...

BugTraq ID: 11508

Remote: Yes

Date Published: Oct 22 2004

Relevant URL: <http://www.securityfocus.com/bid/11508>

Summary:

Ability Server is reported prone to a remote buffer overflow vulnerability. This issue affects the FTP component of the application and arises due to insufficient boundary checks performed by the FTP server.

A successful attack can result in memory corruption leading to a crash, however, if an attacker is able to overwrite sensitive memory addresses, they could execute code on a computer. Arbitrary code execution occurs in the context of the FTP process and may result in unauthorized access to the vulnerable computer.

Ability Server versions 2.34 and prior were identified to be vulnerable to this issue.

III. MICROSOFT FOCUS LIST SUMMARY

NO NEW POSTS FOR THE WEEK 2004-10-19 to 2004-10-26.

IV. NEW PRODUCTS FOR MICROSOFT PLATFORMS

1. Firewall RuleMaker

By: The Net Memetic Pte Ltd

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

Relevant URL: <http://firewall.rulemaker.net>

Summary:

Firewall RuleMaker is a Windows-based firewall configuration version control software product for managers of Cisco PIX and Netscreen firewalls.

2. CAT Cellular Authentication Token and eAuthentication Servic...

By: Mega AS Consulting Ltd

Platforms: Java, Linux, OpenBSD, Os Independent, SecureBSD, Solaris, UNIX, Windows 2000, Windows NT

Relevant URL: <http://www.megaas.co.nz>

Summary:

Low cost, easy to use Two Factor Authentication One Time Password token using the Cellular. Does not use SMS or communication, manages multiple OTP accounts – new technology. For any business that want a safer access to its Internet Services. More information at our site.

We also provide eAuthentication service for businesses that will not buy an Authentication product but would prefer to pay a monthly charge for authentication services from our our CAT Server.

3. KeyCaptor Keylogger

By: Keylogger Software

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

Relevant URL: <http://www.keylogger-software.com/keylogger/keylogger.htm>

Summary:

KeyCaptor is your solution for recording ALL keystrokes of ALL users on your computer! Now you have the power to record emails, websites, documents, chats, instant messages, usernames, passwords, and MUCH MORE!

With our advanced stealth technology, KeyCaptor will not show in your processes list and cannot be stopped from running unless you say so!

4. SpyBuster

By: Remove Spyware

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

Relevant URL: <http://www.remove-spyware.com/spybuster.htm>

Summary:

Our award winning spyware / adware scanner and removal software, SpyBuster will scan your computer for over 4,000 known spyware and adware applications. SpyBuster protects your computer from data stealing programs that can expose your personal information.

SpyBuster scanning technology allows for a quick and easy sweep, so you can resume your work in minutes.

5. FreezeX

By: Faronics Technologies USA Inc

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

Relevant URL: <http://www.faronics.com/html/Freezex.asp>

Summary:

FreezeX prevents all unauthorized programs, including viruses, keyloggers and spy ware from executing. Powerful and secure, FreezeX ensures that any new executable, program, or application that is downloaded, introduced via removable media or the network will never install

6. NeoExec for Active Directory

By: NeoValens

Platforms: Windows 2000, Windows XP

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

Summary:

NeoExec® is an operating system extension for Windows 2000/XP that allows the setting of privileges at the application level rather than at the user level.

NeoExec® is the ideal solution for applications that require elevated privileges to run as the privileges are granted to the application, not the user.

NeoExec® is the only solution on the market capable of modifying at runtime the processes' security context — without requiring a second account as with RunAs and RunAs-derived products.

V. NEW TOOLS FOR MICROSOFT PLATFORMS

1. antinat v0.81

By: Malcolm Smith

Relevant URL: <http://yallara.cs.rmit.edu.au/~malsmith/products/antinat/>

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

Summary:

The Antinat SOCKS Server is a multi-threaded, scalable SOCKS server with a client library for writing proxy-based applications. It supports SOCKS 4, SOCKS 5, authentication, firewalling, UDP, and name resolution.

2. PopMessenger 1.60

By: LeadMind Development

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

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

Summary:

Chat and send text messages and files to anyone on your LAN easily and securely!

3. ByteShelter I 1.0

By: MazZoft NDA

Relevant URL: <http://www.mazzoft.com/bs1.zip>

Platforms: Windows 2000, Windows 95/98

Summary:

This steganography tools lets you conceal data in Outlook e-mail messages and .doc files.

4. DiskInternals Uneraser 2.01

By: Alexey Babenko

Relevant URL: http://diskinternals.com/download/Uneraser_Setup.zip

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

Summary:

DiskInternals Uneraser can recover any deleted file, including documents, photos, mp3 and zip files, or even folders and damaged disks. In addition to HDD, the program supports any type of storage media (music sticks,

SecurityFocus Microsoft: SecurityFocus Microsoft Newsletter #212

cameras, flash drives, USB drives, etc)! It works with encrypted files and helps you undelete file lost because of a virus attack or an employee's malicious behavior. No special skills needed; 100% free to try.

5. DiskInternals NTFS Reader 1.01

By: Alexey Babenko

Relevant URL: http://diskinternals.com/download/NTFS_Reader_Setup.zip

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

Summary:

Provides read access to NTFS disks from Windows 95, 98 and Me. Allows you to save any files to any disk visible on the system or on the network. Supports saving compressed or encrypted files.

While saving, it ignores file security policies. It means that it is possible to access absolutely any file on a NTFS disk from Windows 9x.

6. Airscanner Mobile Firewall 1.0

By: Airscanner Corp

Relevant URL: <http://www.airscanner.com/downloads/fw/amfw.exe>

Platforms: Windows CE

Summary:

A Full–Strength Personal Firewall for Your Windows Mobile/Pocket PC handheld.

Airscanner Mobile Firewall for Windows Mobile Pocket PC is a low–level, bi–directional, packet filtering firewall that examines all incoming and outgoing TCP/IP traffic.

This personal firewall ensures that data is permitted based on access control lists that you select from a set of predefined filters, or from filters that you create yourself.

The firewall parses packets as they come in (or go out)

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: SecurityFocus

Stay up to date. All the latest news, columns, jobs and more in a convenient html newsletter – Even a glimpse of upcoming columns and feature articles! Sign up today!

<http://www.securityfocus.com/htmlnewsletter/subscribe>

