

SecurityFocus Microsoft Newsletter #236

Source: <http://www.derkeiler.com/Mailing-Lists/securityfocus/focus-ms/2005-04/0090.html>

From: Marc Fossi (mfossi_at_securityfocus.com)

Date: 04/13/05

Date: Tue, 12 Apr 2005 22:49:58 -0600 (MDT)

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

SecurityFocus Microsoft Newsletter #236

Need to know what's happening on YOUR network? Symantec DeepSight Analyzer is a free service that gives you the ability to track and manage attacks. Analyzer automatically correlates attacks from various Firewall and network based Intrusion Detection Systems, giving you a comprehensive view of your computer or general network. Sign up today!

http://www.securityfocus.com/sponsor/Symantec_sf-news_041130

I. FRONT AND CENTER

1. Cleaning Up Disclosure

II. MICROSOFT VULNERABILITY SUMMARY

1. PHPMyAdmin Convcharset Cross-Site Scripting Vulnerability
2. PHPNuke Multiple Module Cross-Site Scripting Vulnerabilities
3. Adobe Acrobat Reader ActiveX Control LoadFile Information Di...
4. Early Impact ProductCart Multiple Input Validation Vulnerabi...
5. IBM iSeries AS400 LDAP Server Remote Information Disclosure ...
6. MailEnable SMTP Malformed EHLO Request Denial Of Service Vul...
7. MailEnable IMAP Authenticate Request Buffer Overflow Vulnera...
8. Logics Software LOG-FT Arbitrary File Disclosure Vulnerabili...
9. Logics Software LOG-FT Arbitrary File Disclosure Vulnerabili...
10. Comersus Cart Username Field HTML Injection Vulnerability
11. CommuniGate Pro LIST Unspecified Denial of Service Vulnerabi...
12. PHP-Nuke Your_Account Module Username Cross-Site Scripting V...
13. Microsoft Windows Server 2003 SMB Redirector Local Denial Of...
14. PHP-Nuke Your_Account Module Avatarcategory Cross-Site Scrip...
15. PHP-Nuke Downloads Module Lid Parameter Cross-Site Scripting...
16. Computer Associates eTrust Intrusion Detection System Remote...
17. DameWare Mini Remote Control Server Unspecified Privilege Es...
18. PHP-Nuke Web_Links Module Multiple Cross-Site Scripting Vuln...
19. PHP-Nuke Banners.PHP Cross-Site Scripting Vulnerability
20. MailEnable IMAP Login Request Buffer Overflow Vulnerability
21. IBM Lotus Domino Server Web Service Remote Denial Of Service...
22. Ocean12 Membership Manager Pro Cross-Site Scripting Vulnerab...

23. PHP–Nuke Top Module SQL Injection Vulnerability
24. Ocean12 Membership Manager Pro SQL Injection Vulnerability
25. Network–Client FTP Now Local Password Disclosure Vulnerabili...
26. PHP–Nuke Web_Links Module Multiple SQL Injection Vulnerabili...
27. Microsoft April Advance Notification Unspecified Security Vu...
28. Macromedia ColdFusion MX Updater Remote File Disclosure Vuln...
29. PHP–Nuke Downloads Module Multiple SQL Injection Vulnerabili...
30. AN HTTPD CMDIS.DLL Remote Buffer Overflow Vulnerability
31. AN HTTPD Arbitrary Log Content Injection Vulnerability
32. Maxthon Web Browser Plug–in API Security ID Information Disc...
33. Maxthon Web Browser Plug–in API Directory Traversal Vulnerab...
34. PostNuke Phoenix OP Parameter Remote Cross–Site Scripting Vu...
35. PostNuke Phoenix Module Parameter Remote Cross–Site Scriptin...
36. Microsoft Outlook and Outlook Web Access Source Email Adres...

III. MICROSOFT FOCUS LIST SUMMARY

1. PEAP based 802.1x LAN authentication (Thread)
2. Windows XP SP2 update (Thread)
3. Checking what GPs are in effect (Thread)
4. Windows Server 2003 Service Pack 1 (Thread)
5. I need some information on locking down pc's (Thread)
6. Setting permission (Thread)
7. SecurityFocus Microsoft Newsletter #235 (Thread)
8. Integrating Domain and VPN Login (Thread)

IV. NEW PRODUCTS FOR MICROSOFT PLATFORMS

1. CoreGuard Core Security System
2. KeyCaptor Keylogger
3. SpyBuster
4. FreezeX
5. NeoExec for Active Directory
6. Secrets Protector v2.03

V. NEW TOOLS FOR MICROSOFT PLATFORMS

1. Enig3 1.0.0
2. .NET Security Tool Kit 1.0
3. SecureUML 1.0
4. Validator.NET 1.0
5. ldaupenum 0.02alpha
6. TextKeeper 5.0

VI. BOOK EXCERPTS

VII. UNSUBSCRIBE INSTRUCTIONS

VIII. SPONSOR INFORMATION

I. FRONT AND CENTER

1. Cleaning Up Disclosure

By Mark Rasch

A new federal law requires all U.S. financial institutions to notify their customers when a sensitive database breach has occurred. Newly proposed state laws may go even further.

<http://www.securityfocus.com/columnists/316>

II. MICROSOFT VULNERABILITY SUMMARY

1. PHPMyAdmin Convcharset Cross-Site Scripting Vulnerability

BugTraq ID: 12982

Remote: Yes

Date Published: Apr 03 2005

Relevant URL: <http://www.securityfocus.com/bid/12982>

Summary:

phpMyAdmin is prone to a cross-site scripting vulnerability. This issue is due to a failure in the application to properly sanitize user-supplied input to the 'convcharset' parameter.

phpMyAdmin versions prior to 2.6.2-rc1 are affected by this issue.

2. PHPNuke Multiple Module Cross-Site Scripting Vulnerabilities

BugTraq ID: 12983

Remote: Yes

Date Published: Apr 03 2005

Relevant URL: <http://www.securityfocus.com/bid/12983>

Summary:

PHPNuke is reported prone to multiple cross-site scripting vulnerabilities affecting various modules. The affected modules include 'Search', 'FAQ', and 'Encyclopedia'. The 'banners.php' script is also affected.

An attacker can exploit these issues by creating a malicious link containing HTML and script code and send this link to a vulnerable user. This can allow for theft of cookie-based authentication credentials and other attacks.

PHPNuke 7.6 and prior versions are reportedly affected by these issues.

3. Adobe Acrobat Reader ActiveX Control LoadFile Information Di...

BugTraq ID: 12989

Remote: Yes

Date Published: Apr 04 2005

Relevant URL: <http://www.securityfocus.com/bid/12989>

Summary:

It is reported that the Adobe Acrobat Reader ActiveX control is prone to information disclosure vulnerability. Reports indicate that the Adobe Acrobat Reader ActiveX control, may be employed to disclose the existence of a target file.

Information that is harvested by leveraging this vulnerability may be used to aid in further attacks.

This vulnerability is reported to affect Adobe Acrobat Reader version 7.0 and prior versions.

4. Early Impact ProductCart Multiple Input Validation Vulnerabi...

BugTraq ID: 12990

Remote: Yes

Date Published: Apr 04 2005

Relevant URL: <http://www.securityfocus.com/bid/12990>

Summary:

Multiple input validation vulnerabilities reportedly affect Early Impact ProductCart. These issues are due to a failure of the application to properly sanitize user-supplied input prior to using it to carry out critical actions.

SecurityFocus Microsoft: SecurityFocus Microsoft Newsletter #236

The first set of issues are cross-site scripting vulnerabilities that affect the 'NewCust.asp' script, the 'storelocator_submit.asp' script, the 'techErr.asp' script, and the 'advSearch_h.asp' script.

These issues arise as the application fails to properly sanitize input passed through the offending functions before including it in dynamically generated Web content.

The second set of issues are SQL injection vulnerabilities that affect the 'advSearch_h.asp' script and the 'tarinasworld_butterflyjournal.asp' script. The application includes the value of the offending parameters without sanitization, allowing an attacker to inject SQL syntax and manipulate SQL queries.

An attacker may leverage these issues to carry out cross-site scripting and SQL injection attacks against the affected application. This may result in the theft of authentication credentials, destruction or disclosure of sensitive data, and potentially other attacks.

5. IBM iSeries AS400 LDAP Server Remote Information Disclosure ...

BugTraq ID: 12991

Remote: Yes

Date Published: Apr 04 2005

Relevant URL: <http://www.securityfocus.com/bid/12991>

Summary:

A remote information disclosure issue affects IBM iSeries AS400 LDAP Server. This issue is due to a failure of the application to properly secure sensitive information.

An authenticated attacker may leverage this issue to disclose user names and account information of users in their group. This may facilitate further attacks against the affected server.

6. MailEnable SMTP Malformed EHLO Request Denial Of Service Vul...

BugTraq ID: 12994

Remote: Yes

Date Published: Apr 04 2005

Relevant URL: <http://www.securityfocus.com/bid/12994>

Summary:

MailEnable is prone to a vulnerability that may allow remote attackers to crash the SMTP service. The issue arises when the server handles a malformed EHLO request.

This vulnerability is reported to affect all unpatched versions of MailEnable Enterprise Edition and MailEnable Professional 1.5 and later.

7. MailEnable IMAP Authenticate Request Buffer Overflow Vulnera...

BugTraq ID: 12995

Remote: Yes

Date Published: Apr 04 2005

Relevant URL: <http://www.securityfocus.com/bid/12995>

Summary:

MailEnable is prone to a remotely exploitable stack-based buffer overflow vulnerability. This vulnerability is exposed in the server's IMAP implementation. The issue may be triggered with a malicious 'A001 AUTHENTICATE' request to the IMAP service.

This vulnerability is reported to affect all unpatched versions of MailEnable Enterprise Edition and MailEnable Professional 1.5 and later.

8. Logics Software LOG–FT Arbitrary File Disclosure Vulnerabili...

BugTraq ID: 12997

Remote: Unknown

Date Published: Apr 05 2005

Relevant URL: <http://www.securityfocus.com/bid/12997>

Summary:

LOG–FT is reported prone to an arbitrary file disclosure vulnerability. This issue results from an access validation error and can allow a remote attacker to disclose sensitive data.

It is reported that an attacker can simply issue an HTTP GET request to disclose sensitive files in the context of the affected application.

Information disclosed through this attack may expose sensitive data, which may be used to carry out further attacks against a computer. It is not confirmed whether this issue may also allow an attacker to upload arbitrary files.

9. Logics Software LOG–FT Arbitrary File Disclosure Vulnerabili...

BugTraq ID: 12998

Remote: Yes

Date Published: Apr 05 2005

Relevant URL: <http://www.securityfocus.com/bid/12998>

Summary:

LOG–FT is reported prone to an arbitrary file disclosure vulnerability. This issue results from an access validation error and can allow a remote attacker to disclose sensitive data.

It is reported that an attacker can simply issue a specially crafted HTTP GET request to disclose sensitive files in the context of the affected Web server.

Information disclosed through this attack may expose sensitive data that may be used to carry out further attacks against a computer. It is not confirmed whether this issue may also allow an attacker to upload arbitrary files.

10. Comersus Cart Username Field HTML Injection Vulnerability

BugTraq ID: 13000

Remote: Yes

Date Published: Apr 05 2005

Relevant URL: <http://www.securityfocus.com/bid/13000>

Summary:

Comersus Cart is affected by a remote HTML injection vulnerability.

The problem presents itself when a malicious user enters HTML and script code through the Username field of the affected application. This may facilitate the theft of cookie–based authentication credentials as well as other attacks.

Comersus Cart 6.03 is affected by this issue. Other versions may be vulnerable as well.

11. CommuniGate Pro LIST Unspecified Denial of Service Vulnerabi...

BugTraq ID: 13001

Remote: Yes

Date Published: Apr 05 2005

Relevant URL: <http://www.securityfocus.com/bid/13001>

Summary:

CommuniGate Pro is prone to a denial of service when multipart messages are sent to a list. Successful exploitation could cause the server to crash.

12. PHP-Nuke Your_Account Module Username Cross-Site Scripting V...

BugTraq ID: 13007

Remote: Yes

Date Published: Apr 05 2005

Relevant URL: <http://www.securityfocus.com/bid/13007>

Summary:

It is reported that the PHP-Nuke 'Your_Account' module is affected by a cross-site scripting vulnerability. This issue is due to a failure of the application to properly sanitize user-supplied URI input.

This problem presents itself when malicious HTML and script code is sent to the application through the 'username' parameter of the 'Your_Account' module.

This 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.

This vulnerability is reported to affect PHP-Nuke version 7.6 and previous versions.

13. Microsoft Windows Server 2003 SMB Redirector Local Denial Of...

BugTraq ID: 13008

Remote: No

Date Published: Apr 05 2005

Relevant URL: <http://www.securityfocus.com/bid/13008>

Summary:

A local denial of service vulnerability affects Microsoft Windows Server 2003. This issue is due to a failure of the application to properly handle malformed network data during times of heavy load.

A local attacker may leverage this issue to cause an affected computer to restart or stop responding with a blue screen, effectively denying service to legitimate users.

14. PHP-Nuke Your_Account Module Avatarcategory Cross-Site Scrip...

BugTraq ID: 13010

Remote: Yes

Date Published: Apr 05 2005

Relevant URL: <http://www.securityfocus.com/bid/13010>

Summary:

It is reported that the PHP-Nuke 'Your_Account' module is affected by a cross-site scripting vulnerability. This issue is due to a failure of the application to properly sanitize user-supplied URI input.

This problem presents itself when malicious HTML and script code is sent to the application through the 'Avatarcategory' parameter of the 'Your_Account' module.

This 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.

This vulnerability is reported to affect PHP–Nuke version 7.6 and previous versions.

15. PHP–Nuke Downloads Module Lid Parameter Cross–Site Scripting...

BugTraq ID: 13011

Remote: Yes

Date Published: Apr 05 2005

Relevant URL: <http://www.securityfocus.com/bid/13011>

Summary:

It is reported that the PHP–Nuke 'Downloads' module is affected by a cross–site scripting vulnerability. This issue is due to a failure of the application to properly sanitize user–supplied URI input.

This problem presents itself when malicious HTML and script code is sent to the application through the 'Downloads' module.

This 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.

This vulnerability is reported to affect PHP–Nuke version 7.6 and previous versions.

16. Computer Associates eTrust Intrusion Detection System Remote...

BugTraq ID: 13017

Remote: Yes

Date Published: Apr 05 2005

Relevant URL: <http://www.securityfocus.com/bid/13017>

Summary:

eTrust Intrusion Detection System is reported prone to a remote denial of service vulnerability.

This vulnerability specifically arises due to the improper use of the Microsoft Crypto API function called 'CPIImportKey'. eTrust Intrusion Detection System employs the Microsoft Crypto API functionality without wrapper functions to validate user–supplied input and is susceptible to denial of service attacks.

A successful attack can crash the application by exhausting memory resources. This can facilitate further attacks against the network and the possibility of attacks not being detected.

eTrust Intrusion Detection System 3.0 and 3.0 SP1 are reported vulnerable.

17. DameWare Mini Remote Control Server Unspecified Privilege Es...

BugTraq ID: 13023

Remote: Yes

Date Published: Apr 06 2005

Relevant URL: <http://www.securityfocus.com/bid/13023>

Summary:

DameWare Mini Remote Control Server is prone to a remote privilege escalation vulnerability. Specific details about this vulnerability are not currently available.

This vulnerability was reported to affect all versions of DameWare Mini Remote Control Server prior to 3.80 and 4.9.

18. PHP-Nuke Web_Links Module Multiple Cross-Site Scripting Vuln...

BugTraq ID: 13025

Remote: Yes

Date Published: Apr 06 2005

Relevant URL: <http://www.securityfocus.com/bid/13025>

Summary:

PHP-Nuke is reportedly affected by multiple cross-site scripting vulnerabilities in the Web_Links Module. These issues are due to a failure in the application to properly sanitize user-supplied input.

An attacker may leverage these issues to have arbitrary script code executed in the browser of an unsuspecting user. This may facilitate the theft of cookie-based authentication credentials as well as other attacks.

19. PHP-Nuke Banners.PHP Cross-Site Scripting Vulnerability

BugTraq ID: 13026

Remote: Yes

Date Published: Apr 06 2005

Relevant URL: <http://www.securityfocus.com/bid/13026>

Summary:

PHP-Nuke is reportedly affected by a cross-site scripting vulnerability. This issue is due to a failure in the application to properly sanitize user-supplied input.

An attacker may leverage this issue to have arbitrary script code executed in the browser of an unsuspecting user. This may facilitate the theft of cookie-based authentication credentials as well as other attacks.

20. MailEnable IMAP Login Request Buffer Overflow Vulnerability

BugTraq ID: 13040

Remote: Yes

Date Published: Apr 06 2005

Relevant URL: <http://www.securityfocus.com/bid/13040>

Summary:

MailEnable is prone to a remotely exploitable, stack-based buffer overflow vulnerability. This vulnerability is exposed in the server's IMAP implementation. The issue may be triggered with a malicious 'A001 LOGIN' request to the IMAP service.

21. IBM Lotus Domino Server Web Service Remote Denial Of Service...

BugTraq ID: 13045

Remote: Yes

Date Published: Apr 06 2005

Relevant URL: <http://www.securityfocus.com/bid/13045>

Summary:

A remote denial of service vulnerability affects IBM Lotus Domino Server web service. This issue is due to a failure of the application to properly handle malformed network requests.

IBM has denied that this issue is a vulnerability and they have reported conflicting details regarding it. Please see the referenced IBM technote for more information.

An attacker may leverage this issue to crash the nHTTP.EXE web service, denying service to legitimate users.

22. Ocean12 Membership Manager Pro Cross-Site Scripting Vulnerab...

BugTraq ID: 13046

Remote: Yes

Date Published: Apr 06 2005

Relevant URL: <http://www.securityfocus.com/bid/13046>

Summary:

Ocean12 Membership Manager Pro is reportedly affected by a cross-site scripting vulnerability. This issue is due to a failure in the application to properly sanitize user-supplied input.

An attacker may leverage this issue to have arbitrary script code executed in the browser of an unsuspecting user. This may facilitate the theft of cookie-based authentication credentials as well as other attacks.

23. PHP-Nuke Top Module SQL Injection Vulnerability

BugTraq ID: 13047

Remote: Yes

Date Published: Apr 06 2005

Relevant URL: <http://www.securityfocus.com/bid/13047>

Summary:

PHP-Nuke is prone to an SQL injection vulnerability. This issue arises due to insufficient sanitization of user-supplied input.

This issue may allow a remote attacker to manipulate query logic, potentially leading to unauthorized access to sensitive information such as the administrator password hash or corruption of database data. SQL injection attacks may also potentially be used to exploit latent vulnerabilities in the underlying database implementation.

24. Ocean12 Membership Manager Pro SQL Injection Vulnerability

BugTraq ID: 13049

Remote: Yes

Date Published: Apr 06 2005

Relevant URL: <http://www.securityfocus.com/bid/13049>

Summary:

Ocean12 Membership Manager Pro is reportedly affected by an SQL injection vulnerability. This issue is due to a failure in the application to properly sanitize user-supplied input before using it in an SQL query.

Successful exploitation could result in a compromise of the application, disclosure or modification of data, or may permit an attacker to exploit vulnerabilities in the underlying database implementation.

25. Network-Client FTP Now Local Password Disclosure Vulnerabili...

BugTraq ID: 13052

Remote: No

Date Published: Apr 07 2005

Relevant URL: <http://www.securityfocus.com/bid/13052>

Summary:

FTP Now is reported prone to a vulnerability that can allow an attacker to disclose FTP passwords.

A local attacker can gain access to a file, which contains the credentials in plain text format.

The attacker may then use these credentials to access remote FTP servers and carry out other attacks.

FTP Now 2.6.14 is reported prone, however, it is possible that other versions are affected as well.

26. PHP-Nuke Web_Links Module Multiple SQL Injection Vulnerabili...

BugTraq ID: 13055

Remote: Yes

Date Published: Apr 07 2005

Relevant URL: <http://www.securityfocus.com/bid/13055>

Summary:

The Web_Links module of PHP-Nuke is affected by multiple SQL injection vulnerabilities. These issues are due to a failure in the application to properly sanitize user-supplied input before using it in SQL queries.

Successful exploitation could result in a compromise of the application, disclosure or modification of data, or may permit an attacker to exploit vulnerabilities in the underlying database implementation.

These issues are reported to affect PHP-Nuke version 7.6; earlier versions may also be affected.

27. Microsoft April Advance Notification Unspecified Security Vu...

BugTraq ID: 13056

Remote: Unknown

Date Published: Apr 07 2005

Relevant URL: <http://www.securityfocus.com/bid/13056>

Summary:

Microsoft has released advanced notification that they will be releasing eight security bulletins for Windows on January 11th, 2005. Eight vulnerabilities will be addressed by these security bulletins.

The maximum severity rating of any of these bulletins is 'Critical'.

28. Macromedia ColdFusion MX Updater Remote File Disclosure Vuln...

BugTraq ID: 13060

Remote: Yes

Date Published: Apr 07 2005

Relevant URL: <http://www.securityfocus.com/bid/13060>

Summary:

A remote file disclosure vulnerability affects Macromedia ColdFusion MX. The problem presents itself due to a design error that causes potentially sensitive files to be stored in insecure locations.

An attacker may leverage this issue to gain access to compiled Java class files processed by the affected application server. This may facilitate further attacks and application code disclosure.

29. PHP-Nuke Downloads Module Multiple SQL Injection Vulnerabili...

BugTraq ID: 13061

Remote: Yes

Date Published: Apr 07 2005

Relevant URL: <http://www.securityfocus.com/bid/13061>

Summary:

PHP-Nuke Downloads module is reportedly affected by multiple SQL injection vulnerabilities. These issues are due to a failure in the application to properly sanitize user-supplied input before using it in SQL queries.

Successful exploitation could result in a compromise of the application, disclosure or modification of data, or may permit an attacker to exploit vulnerabilities in the underlying database implementation.

These issues are reported to affect PHP-Nuke version 7.6; earlier versions may also be affected.

30. AN HTTPD CMDIS.DLL Remote Buffer Overflow Vulnerability

BugTraq ID: 13066

Remote: Yes

Date Published: Apr 08 2005

Relevant URL: <http://www.securityfocus.com/bid/13066>

Summary:

AN HTTPD is reported prone to a remote buffer overflow vulnerability.

Specifically, the issue presents itself in 'cmdIS.DLL' which calls the 'GetEnvironmentStrings' function to copy environment variables into a finite sized process buffer.

The attacker can issue a malformed HTTP GET command including excessive data as a value for an affected HTTP header to trigger the overflow. This can lead to arbitrary code execution, allowing the attacker to gain unauthorized access in the context of the Web server.

AN HTTPD 1.42n is reported vulnerable, however, it is possible that other versions are affected as well.

31. AN HTTPD Arbitrary Log Content Injection Vulnerability

BugTraq ID: 13069

Remote: Yes

Date Published: Apr 08 2005

Relevant URL: <http://www.securityfocus.com/bid/13069>

Summary:

AN HTTPD is affected by a vulnerability that may allow remote attacker to inject arbitrary content in to the log file. This issue arises due to a failure of input validation.

Corruption of logs may result in concealing attacks and/or misleading an administrator.

This issue can also be exploited to carry out other attacks such as the execution of certain BAT file commands. This can result in the disclosure of source code and text files.

This issue may also aid in the exploitation of the vulnerability described in BID 13066 (AN HTTPD CMDIS.DLL Remote Buffer Overflow Vulnerability).

AN HTTPD 1.42n is reported vulnerable, however, it is possible that other versions are affected as well.

32. Maxthon Web Browser Plug-in API Security ID Information Disc...

BugTraq ID: 13073

Remote: Yes

Date Published: Apr 08 2005

Relevant URL: <http://www.securityfocus.com/bid/13073>

Summary:

It is reported that the Maxthon Web browser is prone to an information disclosure vulnerability. It is reported that Maxthon Plug-in API's are protected with a security ID. Only a website that has knowledge of a Maxthon Plug-in security ID may invoke the plug-in API. However, it is reported that the Side bar Plug-in stores it's security ID in the Plug-in folder.

It is possible for a remote website to include this file in a script and obtain the Security ID's required to access the API of the Plug-in.

33. Maxthon Web Browser Plug-in API Directory Traversal Vulnerab...

BugTraq ID: 13074

Remote: Yes

Date Published: Apr 08 2005

Relevant URL: <http://www.securityfocus.com/bid/13074>

Summary:

It is reported that the Maxthon Web browser Plug-ins employ 'readFile()' and 'writeFile()' API calls to access files in the Plug-in installation directory. However, reports indicate that it is possible to invoke these API calls to read and write arbitrary files by supplying directory traversal sequences in the path to a target file.

A remote attacker may exploit this issue to read and write files on a target computer with the privileges of a user that is running the vulnerable Web browser.

34. PostNuke Phoenix OP Parameter Remote Cross-Site Scripting Vu...

BugTraq ID: 13075

Remote: Yes

Date Published: Apr 08 2005

Relevant URL: <http://www.securityfocus.com/bid/13075>

Summary:

A remote cross-site scripting vulnerability affects PostNuke. This issue is due to a failure of the application to properly sanitize user-supplied input prior to including it in dynamically generated Web content.

An attacker may leverage this issue to have arbitrary script code executed in the browser of an unsuspecting user. This may facilitate the theft of cookie-based authentication credentials as well as other attacks.

35. PostNuke Phoenix Module Parameter Remote Cross-Site Scriptin...

BugTraq ID: 13076

Remote: Yes

Date Published: Apr 08 2005

Relevant URL: <http://www.securityfocus.com/bid/13076>

Summary:

A remote cross-site scripting vulnerability affects PostNuke. This issue is due to a failure of the application to properly sanitize user-supplied input prior to including it in dynamically generated Web content.

An attacker may leverage this issue to have arbitrary script code executed in the browser of an unsuspecting user. This may facilitate the theft of cookie-based authentication credentials as well as other attacks.

36. Microsoft Outlook and Outlook Web Access Source Email Adres...

BugTraq ID: 13078

Remote: Yes

Date Published: Apr 08 2005

Relevant URL: <http://www.securityfocus.com/bid/13078>

Summary:

Microsoft Outlook and Outlook Web Access clients are reported prone to a weakness that may allow remote attackers to send email with a spoofed address.

It is reported that this issue arises when an attacker sends an e-mail by specifying multiple source email addresses.

This issue may allow an attacker to carry out other attacks by combining this issue with social engineering and phishing attacks. An attacker may also bypass email gateways and send email to users.

III. MICROSOFT FOCUS LIST SUMMARY

1. PEAP based 802.1x LAN authentication (Thread)

Relevant URL:

<http://www.securityfocus.com/archive/88/395481>

2. Windows XP SP2 update (Thread)

Relevant URL:

<http://www.securityfocus.com/archive/88/395480>

3. Checking what GPs are in effect (Thread)

Relevant URL:

<http://www.securityfocus.com/archive/88/395477>

4. Windows Server 2003 Service Pack 1 (Thread)

Relevant URL:

<http://www.securityfocus.com/archive/88/395394>

5. I need some information on locking down pc's (Thread)

Relevant URL:

<http://www.securityfocus.com/archive/88/395385>

6. Setting permission (Thread)

Relevant URL:

<http://www.securityfocus.com/archive/88/395339>

7. SecurityFocus Microsoft Newsletter #235 (Thread)

Relevant URL:

<http://www.securityfocus.com/archive/88/395081>

8. Integrating Domain and VPN Login (Thread)

Relevant URL:

<http://www.securityfocus.com/archive/88/395075>

IV. NEW PRODUCTS FOR MICROSOFT PLATFORMS

1. CoreGuard Core Security System

By: Vormetric

Platforms: AIX, Linux, Solaris, Windows 2000, Windows XP

Relevant URL: <http://www.vormetric.com/products/#overview>

Summary:

CoreGuard System profile

The CoreGuard System is the industry's first solution that enforces acceptable use policy for sensitive digital information assets and protects personal data privacy across an enterprise IT environment. CoreGuard's innovative architecture and completeness of technology provide a comprehensive, extensible solution that tightly integrates all the elements required to protect information across a widespread, heterogeneous enterprise network, while enforcing separation of duties between security and IT administration. At the same time, CoreGuard is transparent to users, applications and storage infrastructures for ease of deployment and system management.

CoreGuard enables customers to:

- * Protect customer personal data privacy and digital information assets
- * Protect data at rest from unauthorized viewing by external attackers and unauthorized insiders
- * Enforce segregation of duties between IT administrators and security administration
- * Ensure host & application integrity * Block malicious code, including zero-day exploits

2. 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!

3. 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.

4. 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

5. 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.

6. Secrets Protector v2.03

By: E-CRONIS

Platforms: Windows 2000, Windows XP

Relevant URL: <http://www.e-cronis.com/download/sp.exe>

Summary:

It's the end of your worries about top-secret data of your company, your confidential files or the pictures from the last party. All these will be hidden beyond the reach of ANY intruder and you will be the only one able to handle them. And what you want to delete will be DELETED. It is the ultimate security tool to protect your sensitive information on PC, meeting the three most important security issues: Integrity, Confidentiality and Availability. This product gives you the features of a "folder locker" and a "secure eraser".

Your secret information is available only through this software and there is no other mean to access it. The information is protected at file system level and it cannot be accidentally deleted or overwritten neither in Safe mode nor in other operating system. This program doesn't make your operating system unstable as other related product do and protects your information from being seen, altered or deleted by an unauthorized user with or without his wish. The program allows you to permanently erase your sensitive data using secure wiping methods leaving no trace of your information. Depending on the selected wiping method your data is unrecoverable using software or even hardware recovery techniques.

V. NEW TOOLS FOR MICROSOFT PLATFORMS

1. Enig3 1.0.0

By: CCC Morocco Team

Relevant URL: <http://www.ccc.ma/sw/enig3/>

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

Summary:

Enig3 is a free cryptography tool that can encrypt/decrypt content/data using your own private generated 128 Bits Enig3-Key, was developed on CCC-Morocco Labs, using the most complex cryptographic methodologies. It uses a Flow-Encoding technique which is done in 3 phases...

2. .NET Security Tool Kit 1.0

By: Foundstone Professional Services

Relevant URL:

http://www.foundstone.com/index.htm?subnav=services/navigation.htm&subcontent=/services/overview_s3i

Platforms: Windows XP

Summary:

The Foundstone S3i .NET Security Toolkit includes tools to help design, develop, and test secure .NET software applications. The toolkit includes Validator.NET, .NETMon, and the SecureUML Template.

3. SecureUML 1.0

By: Foundstone Professional Services

Relevant URL:

http://www.foundstone.com/index.htm?subnav=services/navigation.htm&subcontent=/services/overview_s3i

Platforms: Windows XP

Summary:

The SecureUML Visio template defines a custom Unified Modeling Language (UML) dialect to help system architects build roles based access control systems (RBAC).

4. Validator.NET 1.0

By: Foundstone Professional Services

Relevant URL:

http://www.foundstone.com/index.htm?subnav=services/navigation.htm&subcontent=/services/overview_s3i

Platforms: Windows XP

Summary:

Validator.NET enables developers to programmatically determine user input locations that could be potentially exploited by hackers and provides proactive steps to build data validation routines which are loaded into a protection module. The tool helps eliminate common vulnerabilities such as SQL Injection and Cross-Site Scripting.

5. ldaupenum 0.02alpha

By: Roni Bachar & Sol Zehnwirth

Relevant URL: <https://sourceforge.net/projects/ldaupenum>

Platforms: Linux, Perl (any system supporting perl), Windows 2000, Windows 95/98, Windows NT, Windows XP

Summary:

ldaupenum is a perl script designed to enumerate system and password information from domain controllers using the LDAP service when IPC\$ is locked. The script has been tested on windows and linux.

6. TextKeeper 5.0

By: HardwareCrasher

Relevant URL: <http://members.lycos.co.uk/textkeeper/tkup.zip>

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

Summary:

Encrypts text using numeric combinations and two algorithms, One of the algorithms uses 5 different numeric combinations.

VI. BOOK EXCERPTS

1. Google Hacking for Penetration Testers by Johnny Long (Syngress)

Chapter 8 discusses tracking down Web servers, login portals, and network hardware .

<http://www.securityfocus.com/excerpts/syngress>

2. Buffer Overflow Attacks by James C. Foster (Syngress)

Chapter 7 looks at format string attacks, what they are and how to defend against them.

<http://www.securityfocus.com/excerpts/syngress-1>

3. The Art of Computer Virus Research and Defense, by Peter Szor (Symantec)

Chapter 9 presents the strategies of computer worms in detail.

<http://www.securityfocus.com/excerpts/symantec>

VII. 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.

VIII. SPONSOR INFORMATION

Need to know what's happening on YOUR network? Symantec DeepSight Analyzer is a free service that gives you the ability to track and manage attacks.

Analyzer automatically correlates attacks from various Firewall and network based Intrusion Detection Systems, giving you a comprehensive view of your computer or general network. Sign up today!

http://www.securityfocus.com/sponsor/Symantec_sf-news_041130
