

SecurityFocus Microsoft Newsletter #83

Source: <http://www.derkeiler.com/Mailing-Lists/securityfocus/focus-ms/2002-04/0285.html>

From: Marc Fossi (mfossi@securityfocus.com)

Date: 04/22/02

Date: Mon, 22 Apr 2002 15:01:14 -0600 (MDT)

From: Marc Fossi <mfossi@securityfocus.com>

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

SecurityFocus Microsoft Newsletter #83

This newsletter is sponsored by SecurityFocus (www.securityfocus.com)

Attention Non-profits and Universities: Sign-up now for preferred pricing on the only global early-warning system for cyber attacks – SecurityFocus ARIS Threat Management System.

Click here for more info

<http://www.securityfocus.com/corporate/products/pdpsection.shtml>

I. FRONT AND CENTER

1. VBA Emulation: A Viable Method of Macro Virus Detection? Part One
2. Network Intrusion Detection Signatures, Part Five
3. Closing the Spycam Sniffer Loophole
4. Peddling Snake Oil as Security
5. Cutting-Edge High Tech Crime Fighting: Best Practices...

II. MICROSOFT VULNERABILITY SUMMARY

1. Multiple Microsoft Products for MacOS File URL Buffer Overflow
2. Symantec Raptor / Enterprise Firewall FTP Bounce Vulnerability
3. Microsoft IIS CodeBrws.ASP Source Code Disclosure Vulnerability
4. Microsoft IIS CodeBrws.ASP File Extension Check Out By One
5. Microsoft Internet Explorer History List Script Injection
6. Microsoft Internet Explorer Unicode Character Handling DoS
7. TalentSoft Web+ WML Request Cookie Buffer Overflow Vulnerability
8. Microsoft Windows 2000 Lanman Denial of Service Vulnerability
9. Burning Board URL Parameter Manipulation Vulnerability
10. xNewsletter Form Field Input Validation Vulnerability
11. Microsoft Internet Explorer Dialog Same Origin Policy Bypass
12. Microsoft BackOffice Server Web Administration Authentication
13. PVote Poll Content Manipulation Vulnerability
14. IcrediBB Script Injection Vulnerability
15. Foundstone FScan Banner Grabbing Format String Vulnerability
16. WorkforceROI XPede Unprotected Administrative Facilities...

17. XPede DataSource.ASP Information Disclosure Vulnerability
18. WorkforceROI XPede Weak File Protection Vulnerability
19. WorkforceROI XPede Sprc.ASP SQL Injection Vulnerability...
20. Snitz Forums 2000 Members.ASP SQL Injection Vulnerability
21. PVote Unauthorized Administrative Password Change Vulnerability
22. Symantec Norton Personal Firewall 2002 Fragmented Packet...
23. ColdFusion DOS Device File Request System Information...
24. WorkforceROI XPede Arbitrary Time Sheet Disclosure Vulnerability
25. Demarc PureSecure Authentication Check SQL Injection...
26. Symantec Norton Personal Firewall 2002 Portscan Protection...

III. MICROSOFT FOCUS LIST SUMMARY

1. windows domain question (Thread)
2. windows domain question (Thread)
3. OWA and URLScan (Thread)
4. URLScan 2.5 SRP (Thread)
5. Microsoft Security Bulletin MS01-022 (Thread)
6. Ensuring Disabling/Uninstalation of Windows XP Firewall in LAN
7. Microsoft Cluster in DMZ – Need Advice (Thread)
8. OWA and URLScan (Thread)
9. Ensuring Disabling/Uninstalation of Windows XP Firewall in LAN
10. Win 98 Security (Thread)
11. Microsoft Security Bulletin MS01-022 (Thread)
12. Win 98 Security (Thread)
13. Ensuring Disabling/Uninstalation of Windows XP Firewall in LAN
14. Problem with auto unpacking Hotfixes (from 1 machine only)
15. ms02-018 IS dangerous after all (Thread)
16. Any known issue with 10 April 2002 Cumulative Patch for IIS ?
17. FW: Free HFNetChkPro Invitation (Thread)
18. Fwd: ms02-018 IS dangerous after all (Thread)
19. SSL directory structure issue (Thread)
20. Any known issue with 10 April 2002 Cumulative Patch for IIS ?
21. Any known issue with 10 April 2002 Cumulative Patch for IIS ?
22. Administrivia: Users slam Microsoft Security Analyser (Thread)
23. SSL directory structure issue (Thread)
24. Posters Slam Microsoft Training (Thread)
25. Users slam Microsoft Security Analyser (Thread)
26. Users slam Microsoft Security Analyser (Thread)
27. SecurityFocus Microsoft Newsletter #82 (Thread)
28. Posters Slam Microsoft Training (Thread)
29. URLSCAN error 50 (Thread)
30. Scanning MS DHCP networks. Reading dhcp.mdb (Thread)
31. Scanning MS DHCP networks. Reading dhcp.mdb (Thread)
32. Anyone familiar with bitwise's winsshd? (Thread)
33. VPN / IPSEC (Thread)
34. Peculiar login troubles. (Thread)
35. authentication NTLM (Thread)

IV. NEW PRODUCTS FOR MICROSOFT PLATFORMS

1. Datakey CIP
2. McAfee Internet Security 4.0
3. EventReader

V. NEW TOOLS FOR MICROSOFT PLATFORMS

1. Port Scan Attack Detector (psad) v0.9.7
2. MIMEDefang v2.7
3. EventwatchNT v2.3
4. CHX-I Packet Filter v1.1

VI. SPONSORSHIP INFORMATION

I. FRONT AND CENTER

1. VBA Emulation: A Viable Method of Macro Virus Detection? Part One by Gabor Szappanos

This article is the first in a two-part series that will examine some of the problems that exist with emulation, with the end in mind of determining whether or not it is a realistic anti-virus method.

<http://online.securityfocus.com/infocus/1571>

2. Network Intrusion Detection Signatures, Part 5 by Karen Kent Frederick

This is the fifth and final installment in a series of articles on understanding and developing signatures for network intrusion detection systems. In the previous article, we looked at the topic of protocol analysis, meaning that the intrusion detection system actually understands how various protocols, such as FTP, are supposed to work. We initially looked at protocol analysis as it applied to a single request or response. In this article, we will extend this discussion by looking closely at stateful protocol analysis, which involves performing protocol analysis for an entire connection or session, capturing and storing certain pieces of relevant data seen in the session, and using that data to identify attacks that involve multiple requests and responses.

<http://online.securityfocus.com/infocus/1569>

3. Closing the Spycam Sniffer Loophole by Mark Rasch

Those cheap wireless video cameras hawked by annoying pop-up ads can be intercepted by anyone with a few hundred dollars and a voyeuristic bent. There's no federal law against it, but there should be.

<http://online.securityfocus.com/columnists/76>

4. Peddling Snake Oil as Security Richard Forno

Recently, I received an invitation to speak at a plenary session for an upcoming conference on wireless security. While the conference venue was first-rate and they were covering all my expenses, I had to be honest with the conference coordinators and decline the invitation.

<http://online.securityfocus.com/columnists/75>

5. Cutting-Edge High Tech Crime Fighting: Best Practices in Computer Forensics

June 17-18, 2002

American Management Association, Washington, DC

Walk away able to perform computer forensic examinations that will not only yield sound evidence but will also hold up in a court of law! Learn to find, collect and preserve digital evidence, and present the evidence in court. Also learn to successfully combine private and public computer forensics forces to investigate computer crimes. Keynote speech by Microsoft's Chief Security Strategist Scott Charney. Public sector employee discounts available.

For more information, call 800-280-8440, or visit www.frallc.com (see InfoTech events).

II. BUGTRAQ SUMMARY

1. Multiple Microsoft Products for MacOS File URL Buffer Overflow Vulnerability

BugTraq ID: 4517

Remote: Yes

Date Published: Apr 16 2002 12:00A

Relevant URL:

<http://www.securityfocus.com/bid/4517>

Summary:

An issue has been reported in various Microsoft products for MacOS, including Internet Explorer, Outlook Express, Entourage, PowerPoint, Excel and Word.

Reportedly, a common component of all of the listed products contain a buffer overflow condition. The problem exists in the handling of file:/// URLs.

If an attacker creates a file:/// URL containing arbitrary data (approx 1313 bytes) and indexing at least one subdirectory, upon a user accessing the maliciously crafted link, the arbitrary data will execute and potentially initiate the overflow. For example:

file:///arbitrary_data or <file:///data/data/data/data/>

This overflow could overwrite stack variables, including the return address, and be used to execute arbitrary code with the privilege level of the user. However, sending random data could cause the application to crash.

2. Symantec Raptor / Enterprise Firewall FTP Bounce Vulnerability

BugTraq ID: 4522

Remote: Yes

Date Published: Apr 16 2002 12:00A

Relevant URL:

<http://www.securityfocus.com/bid/4522>

Summary:

Raptor Firewall is an enterprise level firewall originally developed by Axent Technologies and is maintained and distributed by Symantec. Symantec Enterprise Firewall is formerly known as Raptor firewall. It is available for Microsoft Windows and Unix operating systems.

Some FTP implementations allow for the FTP PORT command to be used to send data from the server to a host other than the client. This well documented weakness in the protocol is known as the FTP Bounce Attack. It is fixed in most modern FTP servers.

The Raptor Firewall implementation of the FTP protocol is susceptible to FTP bounce attacks.

Raptor Firewall rewrites the headers of incoming and outbound packets in such a way as to make the FTP bounce attacks possible. When a FTP PORT command is parsed by the vulnerable firewall, the IP address in the command is changed to the attacker's and the port is changed to a number in the ephemeral port range. To the FTP server behind the firewall, this is a permissible PORT request.

However, when the firewall handles the resultant outgoing connection made by the FTP server, the IP address and port of the command are replaced with the original attacker supplied values.

Consequently, the attacker can cause the data to be sent to an arbitrary host.

It should be noted that affected firewall implementations disable FTP PORT connections to ports below 1024.

Symantec has reported that Enterprise Firewall V7.0 for Solaris is also vulnerable to this issue.

3. Microsoft IIS CodeBrws.ASP Source Code Disclosure Vulnerability

BugTraq ID: 4525

Remote: Yes

Date Published: Apr 16 2002 12:00A

Relevant URL:

<http://www.securityfocus.com/bid/4525>

Summary:

Microsoft IIS 5.0 ships with a sample script that may be used to view the source code of other scripts in the sample scripts (/IISSAMPLES) directory.

The vulnerable script (CodeBrws.asp) makes an attempt to filter standard attempts to break out of the sample scripts directory using dot-dot-slash directory traversal attacks. However, this script does not adequately filter unicode representations of directory traversals. For example, an attacker can break out of the sample script directory by substituting '%c0%ae%c0%ae' for '..' in a dot-dot-slash directory traversal attack.

Disclosure of script source code may reveal sensitive information to an attacker. Plaintext database credentials are often contained in script source code. Additionally, the attacker may exploit this condition to search for other more serious vulnerabilities that may exist in scripts on the host running the vulnerable software.

It has been demonstrated that this issue may be exploited to map out the directory structure of the filesystem on a host running the vulnerable script. This script, when attempting to view the source code for a file, gives feedback as to the user as to whether the file/directory exists or not. For example, a request for a non-existent directory returns a "Path not found" response. A request for a non-existent file in an existing directory returns a "File not found" response.

4. Microsoft IIS CodeBrws.ASP File Extension Check Out By One Vulnerability BugTraq ID: 4543

Remote: Yes

Date Published: Apr 18 2002 12:00A

Relevant URL:

<http://www.securityfocus.com/bid/4543>

Summary:

Microsoft IIS 5.0 ships with a sample script that may be used to view the source code of other scripts in the sample scripts (/IISSAMPLES) directory.

The vulnerable script (CodeBrws.asp) validates user input to ensure that any file viewed has one of a select set of file extensions, namely .html, .htm, .asp and .inc. This check is performed by testing a substring taken from the end of the requested file path.

An out by one error has been reported in this check. The section of the path tested is larger than required. As a result, provided file extensions may include an additional character and still pass the test. For example, .aspx files used by the .NET architecture may also be viewed. This may allow an attacker to view sensitive information contained in files not believed to be exposed.

If used in conjunction with the issues discussed in BID 4525, this may expose files outside of the sample script directory.

5. Microsoft Internet Explorer History List Script Injection Vulnerability BugTraq ID: 4505

Remote: Yes

Date Published: Apr 15 2002 12:00A

Relevant URL:

<http://www.securityfocus.com/bid/4505>

Summary:

A vulnerability has been reported in some versions of Internet Explorer. It is possible to inject JavaScript code into the browser history list, and execute it within any page context given appropriate user interaction.

Internet Explorer stores javascript: URLs in the browser history list. Script executed within the javascript: URL will inherit the security zone of the last viewed page. This provides protection against javascript: URLs included within a maliciously constructed web page. However, a user may navigate to a javascript: URL using the 'Back' button in their browser. This may result in the injected script code executing within the context of another page.

It is possible to construct a javascript: URL which will detect the usage of the 'Back' button, and behave differently under these conditions. This allows an attacker to construct a javascript: URL which will initially redirect the user to an arbitrary location, then perform additional actions when the 'Back' button is used. This can result in arbitrary script executing within an arbitrary context, so long as the user behaves as anticipated.

Exploitation of this vulnerability can result in JavaScript code executing within the context of an arbitrary site, or within the Local Computer context. This can result in the disclosure of cookie data or local file contents.

This behavior has been reported in versions 6.0 and 5.5 of IE. Other versions of Internet Explorer may share this vulnerability. This has not, however, been confirmed.

6. Microsoft Internet Explorer Unicode Character Handling DoS Vulnerability

BugTraq ID: 4519

Remote: Yes

Date Published: Apr 16 2002 12:00A

Relevant URL:

<http://www.securityfocus.com/bid/4519>

Summary:

It has been reported that Microsoft Internet Explorer crashes when accessing a URL containing an excessive number of unicode characters. This condition may reportedly be triggered if the web user clicks on a maliciously constructed link containing an excessive number of unicode characters. The attacker would essentially have to entice the user into submitting the URL with a vulnerable web browser.

It is not known what causes this to occur. It may not be possible to reproduce this issue on all environments, including two different systems running the same version of the Microsoft Windows operating system with the same version of Internet Explorer. The exact circumstances of why this issue occurs in some environments and not in others are not known at this time.

It has been suggested that this vulnerability is caused by a buffer overflow condition.

This record will be updated as more information becomes available.

7. TalentSoft Web+ WML Request Cookie Buffer Overflow Vulnerability

BugTraq ID: 4530

Remote: Yes

Date Published: Apr 17 2002 12:00A

Relevant URL:

<http://www.securityfocus.com/bid/4530>

Summary:

TalentSoft Web+ is an environment for developing web-based client/server applications. It will run on Microsoft Windows 9x/NT/2000 and Unix operating systems.

An exploitable buffer overflow has been discovered in Web+ when an oversized cookie is sent with a request for a WML file. This overflow could overwrite stack variables, including the return address, and be used to execute arbitrary code as the web server process. However, sending random data could cause the application to crash.

As the Web+ service runs with SYSTEM privileges under IIS 4, exploitation of arbitrary code will enable a remote attacker to fully compromise a host running the vulnerable software. Under IIS 5, IWAM_* privileges may be obtained with lesser consequences. Regardless, however, exploitation may allow local access to the vulnerable system.

8. Microsoft Windows 2000 Lanman Denial of Service Vulnerability

BugTraq ID: 4532

Remote: Yes

Date Published: Apr 17 2002 12:00A

Relevant URL:

<http://www.securityfocus.com/bid/4532>

Summary:

An issue has been discovered in Windows 2000, which could cause a denial of system services.

Submitting malformed data to port 445 could cause the Lanman service to consume high CPU and Kernel mode memory usage.

A restart of the server may be required in order to regain normal functionality. Although reports indicate that in extreme cases administrators have received the error message "You do not have permissions to shutdown or restart this computer."

9. Burning Board URL Parameter Manipulation Vulnerability

BugTraq ID: 4512

Remote: Yes

Date Published: Apr 15 2002 12:00A

Relevant URL:

<http://www.securityfocus.com/bid/4512>

Summary:

Burning Board is web forum software. It is written in PHP, back-ended by MySQL, and will run on most Unix and Linux variants as well as Microsoft Windows.

An attacker may allegedly create a malicious link which is capable of causing actions to be performed on the behalf of a legitimate Burning Board user who visits the link. To exploit this vulnerability, the attacker must manipulate URL parameters in the malicious link in such a way as to cause the desired actions to be performed by a user who visits the link. The legitimate forum user must also be authenticated via a cookie-based authentication credential. The link may include BBCode.

If the attacker launches this attack via a malicious attacker-controlled webpage, then it is trivial for the attacker to write a script to conceal that unauthorized actions have been performed on the behalf of the legitimate user. The attacker's script would most likely redirect the user to an expected webpage after the attack has been performed. Otherwise, it is possible the user may discover that an attempt has been made to perform actions on their behalf.

This might be exploited by an attacker to cause an arbitrary attacker-supplied forum message to be posted by a legitimate user who visits the malicious webpage.

It has been reported, but not confirmed, that other web forum software (such as phpBB) may also be affected by this vulnerability.

10. xNewsletter Form Field Input Validation Vulnerability

BugTraq ID: 4516

Remote: Yes

Date Published: Apr 14 2002 12:00A

Relevant URL:

<http://www.securityfocus.com/bid/4516>

Summary:

xNewsletter is a script that allows web users to subscribe to a newsletter. It is written in PHP and will run on most Unix and Linux variants, as well as Microsoft Windows operating systems.

xNewsletter does not sanitize dangerous characters from form field input such as the e-mail address of the newsletter recipient.

It has been demonstrated that this condition may be exploited to cause multiple instances of the same e-mail address to be written to the datafile. For example, the "%" character is used to separate e-mail addresses in the datafile. If this character is included as part of an e-mail address, the script assumes that it is a new e-mail address and does not check to see if the e-mail address already exists in the datafile. Multiple instances of the same address can be added by using the "%" character to separate each instance. An attacker may effectively trick the script into mail bombing an arbitrary e-mail address.

It has also been demonstrated that PHP code may be included to enable the attacker may cause arbitrary data to be written to the datafile in such a way that it cannot be removed using the facilities provided by xNewsletter. The malformed data must be removed from the datafile manually.

It may also be possible, under some circumstances, to execute remote commands via the inclusion of attacker-supplied PHP code. Though this possibility has not been confirmed.

These two consequences of insufficient validation of form input may be exploited in conjunction with each other.

11. Microsoft Internet Explorer Dialog Same Origin Policy Bypass Vulnerability

BugTraq ID: 4527

Remote: Yes

Date Published: Apr 16 2002 12:00A

Relevant URL:

<http://www.securityfocus.com/bid/4527>

Summary:

It is possible to bypass the origin policy used by Internet Explorer for the showModalDialog and showModelessDialog functions. Under some circumstances, it may be possible to execute script code in sensitive contexts.

Microsoft Internet Explorer includes support for dialog windows through script calls to the two functions showModalDialog and showModelessDialog. These functions accept a URL location for the dialog content, and an option argument parameter to allow data to be passed to the dialog from the calling page.

A check is done to ensure that data is only passed to dialogs located in the same domain, port and protocol as the calling page. This prevents a malicious party from injecting content into arbitrary dialogs. However, if the URL provided as the dialog source redirects to a second location, only the first is subject to this security check.

As a result, a malicious party may open a dialog with a URL which will pass this check, and then redirect the dialog to an arbitrary file. The security check will be passed based on the initial provided location, and attacker supplied data will be passed to the second dialog.

The consequences of exploitation are highly dependant on the functionality of the targetted dialog. It is likely that this vulnerability could lead to subversion of information or social engineering attacks.

It has been demonstrated to possibly inject script code into dialogs included by default with versions of Internet Explorer 5.0, 5.5 and 6.0. This can be used to execute arbitrary script code in the local computer context.

12. Microsoft BackOffice Server Web Administration Authentication Bypass Vulnerability

BugTraq ID: 4528

Remote: Yes

Date Published: Apr 17 2002 12:00A

Relevant URL:

<http://www.securityfocus.com/bid/4528>

Summary:

Microsoft BackOffice suite of products include a web based administration ASP based application that runs on IIS. The BackOffice Web Administrator component of BackOffice Server contains a design flaw, which could allow for unauthorized users to bypass authentication.

This is achieved when submitting an HTTP request directly to services.asp (Boadmin/Backoffice/Services.asp). No credentials are required to enter the administration page, and such a request will bypass the login screen.

It should be noted that this issue only occurs if basic authentication is being used. In addition by default, the BackOffice Web Administrator is configured to accept connections only from the Localhost (127.0.0.1). However, it is likely that administrators have changed this setting in order to use the administration interface for remote access.

13. PVote Poll Content Manipulation Vulnerability

BugTraq ID: 4540

Remote: Yes

Date Published: Apr 18 2002 12:00A

Relevant URL:

<http://www.securityfocus.com/bid/4540>

Summary:

PVote is a web voting system written in PHP. It will run on most Unix and Linux variants as well as Microsoft Windows operating systems.

It is possible for a remote attacker to add/delete web polls just by manipulating the values of URL parameters. No authentication credentials

are required for the attacker to perform these actions. This may enable a remote attacker to manipulate some of the content on a website running the voting system.

14. IcrediBB Script Injection Vulnerability

BugTraq ID: 4548

Remote: Yes

Date Published: Apr 19 2002 12:00A

Relevant URL:

<http://www.securityfocus.com/bid/4548>

Summary:

IcrediBB is freely available web forum software. It is written in PHP and will run on most Unix and Linux variants, as well as Microsoft Windows operating systems.

IcrediBB does not adequately filter HTML tags from forum message form fields. This may enable an attacker to inject malicious script code into forum messages. In particular, script code is not sufficiently sanitized from the thread title and body form fields. When a web user views a message containing the attacker's script code, the malicious script code is executed in their browser, in the security context of the website running the vulnerable software.

An attacker who exploits this may be able to hijack web content or steal cookie-based authentication credentials.

15. Foundstone FScan Banner Grabbing Format String Vulnerability

BugTraq ID: 4549

Remote: Yes

Date Published: Apr 19 2002 12:00A

Relevant URL:

<http://www.securityfocus.com/bid/4549>

Summary:

FScan is the commercially available network scanning utility distributed and maintained by Foundstone. This problem affects the version available for the Microsoft Windows platform.

A problem with the software package could make it possible to remotely execute code on a vulnerable host. The problem is in the banner-grabbing function of the software.

Under some circumstances, it may be possible to execute arbitrary code on a scanning host. This is due to FScan not properly handling banner data supplied by scanned hosts when the scanner is executed against them. This problem is the result of a format string vulnerability, and could lead to the overwriting arbitrary locations in memory, and execution of attacker supplied code.

This vulnerability may only be exploited when the FScan software has been configured to grab banners from scanned hosts. The attacker must place the exploit string in the banner of a host which will be scanned by FScan. The result is the execution of code with the privileges of the user running the FoundScan program.

16. WorkforceROI XPede Unprotected Administrative Facilities Vulnerability

BugTraq ID: 4552

Remote: Yes

Date Published: Apr 19 2002 12:00A

Relevant URL:

<http://www.securityfocus.com/bid/4552>

Summary:

XPede is web-based project accounting software. It is available for Microsoft Windows operating systems.

XPede does not prompt non-administrative users for administrative authentication credentials if they attempt to access an administrative script. This may enable a malicious XPede user to gain unauthorized access to the administrative facilities of the software. For example, the malicious user may access the '/admin/adminproc.asp' script to enumerate/add/delete other users of the XPede project accounting system.

Successful exploitation would require the attacker to know the name/location of administrative scripts.

This issue was reported for XPede 4.1. Other versions may also be affected.

17. XPede DataSource.ASP Information Disclosure Vulnerability

BugTraq ID: 4553

Remote: Yes

Date Published: Apr 19 2002 12:00A

Relevant URL:

<http://www.securityfocus.com/bid/4553>

Summary:

XPede is web-based project accounting software. It is available for Microsoft Windows operating systems.

XPede uses Microsoft SQL Server to store its data.

When the XPede datasource.asp script is accessed it displayed a HTML form that contains the database user name. This script may be accessed by arbitrary web users without requiring any sort of authentication.

Additionally, the script provides an interface for changing the user's password. To change the password, the current password must be provided. However, since this interface is exposed and the database user name has also been disclosed, this may provide an attacker with an opportunity to

brute-force the password of the database user.

This issue was reported for XPede 4.1. Other versions may also be affected.

18. WorkforceROI XPede Weak File Protection Vulnerability

BugTraq ID: 4554

Remote: Yes

Date Published: Apr 19 2002 12:00A

Relevant URL:

<http://www.securityfocus.com/bid/4554>

Summary:

XPede is web-based project accounting software. It is available for Microsoft Windows operating systems.

When a user submits an expense claim, the file is saved in the world-readable '/reports/temp' directory. By default this directory is indexable. Remote clients may be able to access the temporary reports of other users by accessing this directory.

Furthermore, the files may still be obtained if indexing has been disabled for the '/reports/temp' directory. For security reasons, the filenames assigned are partially random. Unfortunately the scheme is weak: the random component of the filename is only 5 bytes in length and limited to alpha-numeric characters. This makes the space of possible filenames relatively small and easily exhausted by an automated guessing utility.

As a result, it may be possible for a user to obtain sensitive information which could assist in social engineering attacks.

This issue was reported for XPede 4.1. Other versions may also be affected.

19. WorkforceROI XPede Sprc.ASP SQL Injection Vulnerability

BugTraq ID: 4555

Remote: Yes

Date Published: Apr 19 2002 12:00A

Relevant URL:

<http://www.securityfocus.com/bid/4555>

Summary:

XPede is web-based project accounting software. It is available for Microsoft Windows operating systems.

XPede is back-ended by Microsoft SQL Server.

A vulnerability in the XPede sprc.asp script makes it possible for a malicious user to launch SQL injection attacks. The vulnerable script contains an option entitled "Qry", which may enable the attacker to

inject a literal SQL query, which will be executed by the underlying database. This may be possibly be exploited to list database tables or modify/delete data. User and administrative authentication credentials are stored in the database, in addition to other types of project accounting related information.

Vulnerabilities or misconfigurations in the underlying database might also be exploited via this issue.

This issue was reported for XPede 4.1. Other versions may also be affected.

20. Snitz Forums 2000 Members.ASP SQL Injection Vulnerability

BugTraq ID: 4558

Remote: Yes

Date Published: Apr 19 2002 12:00A

Relevant URL:

<http://www.securityfocus.com/bid/4558>

Summary:

Snitz Forums 2000 is ASP-based web forum software. It runs on Microsoft Windows operating systems. Snitz is back-ended by a database and supports Microsoft Access 97/2000, SQL Server 6.5/7.0/2000 and MySQL.

Snitz Forums 2000 includes a feature that allows users to get a listing of the registered users of the web forum. To accomplish this, the members.asp script constructs a query to the underlying database for a list of registered users.

However, it is possible for a remote attacker to inject SQL into queries made by the members.asp script. This may be exploited to manipulate the logic of a query made by the script.

Depending on the database implementation used, this may possibly result in sensitive information in the database being disclosed to the attacker or may enable the attacker to modify data. There is also the possibility that this issue may be leveraged to exploit vulnerabilities that may exist in the underlying database.

The attacker would have to pass properly formatted SQL to the vulnerable script to exploit this issue.

21. PVote Unauthorized Administrative Password Change Vulnerability

BugTraq ID: 4541

Remote: Yes

Date Published: Apr 18 2002 12:00A

Relevant URL:

<http://www.securityfocus.com/bid/4541>

Summary:

PVote is a web voting system written in PHP. It will run on most Unix and Linux variants as well as Microsoft Windows operating systems.

It is possible to change the administrative password by submitting a malicious web request. The attacker does not require the old administrative password to change the new one. The structure of such a malicious web request is as follows:

http://target/pvote/ch_info.php?newpass=password

The ch_info.php script will accept arbitrary attacker-supplied values for the newpass and confirm values without requiring any sort of authentication.

22. Symantec Norton Personal Firewall 2002 Fragmented Packet Vulnerability

BugTraq ID: 4545

Remote: Yes

Date Published: Apr 16 2002 12:00A

Relevant URL:

<http://www.securityfocus.com/bid/4545>

Summary:

Symantec Norton Personal Firewall 2002 (NPW) is a firewall for home and small office machines based on some versions of the Microsoft Windows operating systems.

It has been reported that NPW may not adequately filter packet fragments. In particular, denial of service attacks based on fragmented packets have been reported to work effectively against systems protected by NPW. This may happen even if the attacking address is entirely blocked from the system.

Reportedly, this occurs with the block fragmented IP packets feature enabled.

This may expose protected machines to attacks, in the event that other software vulnerabilities exist. Further information on the nature of this issue is not currently available.

These issues have not been confirmed.

23. ColdFusion DOS Device File Request System Information Disclosure Vulnerability

BugTraq ID: 4542

Remote: Yes

Date Published: Apr 18 2002 12:00A

Relevant URL:

<http://www.securityfocus.com/bid/4542>

Summary:

Allaire Macromedia ColdFusion is a web application server. This issue impacts versions of ColdFusion for the Microsoft Windows family of

operating systems.

Submitting a web request for certain non-existent .cfm or .dbm files will cause the ColdFusion host to return an error message containing the path to the web root. This has also been known to occur when submitting a request for a DOS-device (CON, AUX, PRN, NUL) with either a .cfm or .dbm extension.

Successful exploitation of this issue will give an attacker sensitive information about the system configuration, and may allow further, intelligent attacks.

24. WorkforceROI XPede Arbitrary Time Sheet Disclosure Vulnerability

BugTraq ID: 4556

Remote: Yes

Date Published: Apr 19 2002 12:00A

Relevant URL:

<http://www.securityfocus.com/bid/4556>

Summary:

XPede is web-based project accounting software. It is available for Microsoft Windows operating systems.

An issue has been reported in XPede which could allow a remote user to access the time sheets of other users. The vulnerability is in the 'ets_app_process.asp' script and is due to a lack of adequate authorization checks. It is possible for remote attackers to obtain user timesheets by simply modifying the incrementally assigned TSN id script parameter. If a timesheet exists with the attacker-supplied ID number, it will be output to the client.

As a result, unauthorized users could reveal sensitive user information. This information may be used to assist in social engineering attacks.

This issue was reported for XPede 4.1. Other versions may also be affected.

25. Demarc PureSecure Authentication Check SQL Injection Vulnerability

BugTraq ID: 4520

Remote: Yes

Date Published: Apr 15 2002 12:00A

Relevant URL:

<http://www.securityfocus.com/bid/4520>

Summary:

Demarc PureSecure is a commercially available graphical front-end for Snort, in addition to being a generalized network monitoring solution. Snort is an open-source NIDS (Network Intrusion Detection System). Demarc PureSecure will run on most Linux and Unix variants, as well as Microsoft Windows NT/2000/XP operating systems.

A vulnerability has been reported in some versions of PureSecure. User supplied input is used to construct a SQL statement, allowing SQL injection attacks. Administrative access may be gained through exploitation of this flaw.

A session id value is derived from cookie information, which is under the control of the client. This information is then used to construct a SQL query, which is used to determine if the user has administrative access. A malicious attacker may construct a cookie including additional SQL commands, and modify this query.

It has been reported possible to gain administrative access through this attack. Further exploitation may be possible, although this has not been confirmed.

26. Symantec Norton Personal Firewall 2002 Portscan Protection Bypass Vulnerability

BugTraq ID: 4521

Remote: Yes

Date Published: Apr 16 2002 12:00A

Relevant URL:

<http://www.securityfocus.com/bid/4521>

Summary:

Symantec Norton Personal Firewall 2002 (NPW) is a firewall solution for home and small office machines based on some versions of the Microsoft Windows operating systems. It has a variety of features, including the ability to detect and dynamically block portscans.

An issue has been reported with the manner in which Personal Firewall 2002 handles portscans. Reportedly, only SYN scans are detected. An attacker may scan with a variety of other methods, including SYN/FIN packets and evade the protective features of NPW.

Additionally, when a scan is protected it has been reported that only incoming SYN packets from the attacking address are blocked. The attacker may continue to probe the target machine with the methods mentioned above, and currently open connections are not dropped.

It has also been reported that the 30 minute blacklist time for portscan protection is not configurable. This may allow the attacker to fingerprint the system as running NPW 2002, possibly allowing for further intelligent attacks.

III. MICROSOFT FOCUS LIST SUMMARY

1. windows domain question (Thread)

Relevant URL:

[6e00010a@lauradominion.com">http://online.securityfocus.com/archive/88/16bf01c1e7de\\$9a87c6b0\\$6e00010a@lauradominion.com](http://online.securityfocus.com/archive/88/16bf01c1e7de$9a87c6b0$6e00010a@lauradominion.com)

SecurityFocus Microsoft: SecurityFocus Microsoft Newsletter #83

2. windows domain question (Thread)

Relevant URL:

[20020419195940.15928.qmail@web10701.mail.yahoo.com](http://online.securityfocus.com/archive/88/20020419195940.15928.qmail@web10701.mail.yahoo.com)">http://online.securityfocus.com/archive/88/20020419195940.15928.qmail@web10701.mail.yahoo.com

3. OWA and URLScan (Thread)

Relevant URL:

[5.1.0.14.2.20020419112334.03229598@mail.hammerofgod.com](http://online.securityfocus.com/archive/88/5.1.0.14.2.20020419112334.03229598@mail.hammerofgod.com)">http://online.securityfocus.com/archive/88/5.1.0.14.2.20020419112334.03229598@mail.hammerofgod.com

4. URLScan 2.5 SRP (Thread)

Relevant URL:

[9AACD631D86FD51182C500306E02085801E014BB@asbut116.asb.countrycompanies.com](http://online.securityfocus.com/archive/88/9AACD631D86FD51182C500306E02085801E014BB@asbut116.asb.countrycompanies.com)">http://online.securityfocus.com/archive/88/9AACD631D86FD51182C500306E02085801E014BB@asbut116.asb.countrycompanies.com

5. Microsoft Security Bulletin MS01-022 (Thread)

Relevant URL:

[A4E79859B1467D4EB5CCC7FD149A454A43B10C@adsroot.bsihq.com](http://online.securityfocus.com/archive/88/A4E79859B1467D4EB5CCC7FD149A454A43B10C@adsroot.bsihq.com)">http://online.securityfocus.com/archive/88/A4E79859B1467D4EB5CCC7FD149A454A43B10C@adsroot.bsihq.com

6. Ensuring Disabling/Uninstallation of Windows XP Firewall in LAN enviro. (Thread)

Relevant URL:

[98C26F3827C1D511AE6200508BCF2442C4E1BE@milntex1.rwbaird.com](http://online.securityfocus.com/archive/88/98C26F3827C1D511AE6200508BCF2442C4E1BE@milntex1.rwbaird.com)">http://online.securityfocus.com/archive/88/98C26F3827C1D511AE6200508BCF2442C4E1BE@milntex1.rwbaird.com

7. Microsoft Cluster in DMZ – Need Advice (Thread)

Relevant URL:

[C36A1205AC70474190A53329067EBF7E2680F6@ponyx.safecu.org](http://online.securityfocus.com/archive/88/C36A1205AC70474190A53329067EBF7E2680F6@ponyx.safecu.org)">http://online.securityfocus.com/archive/88/C36A1205AC70474190A53329067EBF7E2680F6@ponyx.safecu.org

8. OWA and URLScan (Thread)

Relevant URL:

<http://online.securityfocus.com/archive/88/859A11E09843BC48A67C176D12E38857337619@BMA-EXCHANGE->

9. Ensuring Disabling/Uninstallation of Windows XP Firewall in LAN enviro. (Thread)

Relevant URL:

[5.1.0.14.2.20020419073819.0324d118@mail.hammerofgod.com](http://online.securityfocus.com/archive/88/5.1.0.14.2.20020419073819.0324d118@mail.hammerofgod.com)">http://online.securityfocus.com/archive/88/5.1.0.14.2.20020419073819.0324d118@mail.hammerofgod.com

10. Win 98 Security (Thread)

Relevant URL:

<http://online.securityfocus.com/archive/88/F50520282C60D511849600306E07D1CA4A6E8D@MGEX1>

11. Microsoft Security Bulletin MS01-022 (Thread)

Relevant URL:

[3CC0279E.CEFF5D2C@espgroup.net](http://online.securityfocus.com/archive/88/3CC0279E.CEFF5D2C@espgroup.net)">http://online.securityfocus.com/archive/88/3CC0279E.CEFF5D2C@espgroup.net

12. Win 98 Security (Thread)

Relevant URL:

[3CBFE840.7040301@aldigital.co.uk">http://online.securityfocus.com/archive/88/3CBFE840.7040301@aldigital.co.u](http://online.securityfocus.com/archive/88/3CBFE840.7040301@aldigital.co.uk)

13. Ensuring Disabling/Uninstalation of Windows XP Firewall in LAN enviro. (Thread)

Relevant URL:

[http://online.securityfocus.com/archive/88/001301c1e73b\\$e8f28860\\$a78386cb@hedni01](http://online.securityfocus.com/archive/88/001301c1e73b$e8f28860$a78386cb@hedni01)

14. Problem with auto unpacking Hotfixes (from 1 machine only) (Thread)

Relevant URL:

[761DBCC144B6334A81251171C684A6FB73C562@mailserver-2k.fireapple.com">http://online.securityfocus.com/a](http://online.securityfocus.com/a761DBCC144B6334A81251171C684A6FB73C562@mailserver-2k.fireapple.com)

15. ms02-018 IS dangerous after all (Thread)

Relevant URL:

<http://online.securityfocus.com/archive/88/120097989CFFD1118B8C00805FFEE24608C0BE7B@GBWTM001>

16. Any known issue with 10 April 2002 Cumulative Patch for IIS ? (Thread)

Relevant URL:

[F09AE4CA8CCD6A4DA1C2A17F50E27F0A05B6A2@des.avet.com.pl">http://online.securityfocus.com/archive/88/](http://online.securityfocus.com/archive/88/F09AE4CA8CCD6A4DA1C2A17F50E27F0A05B6A2@des.avet.com.pl)

17. FW: Free HFNetChkPro Invitation (Thread)

Relevant URL:

[CIEFJFMPGJFJLBIBHPAGEFEKKA.dadams@scientech.com">http://online.securityfocus.com/archive/88/CIEFJ](http://online.securityfocus.com/archive/88/CIEFJFMPGJFJLBIBHPAGEFEKKA.dadams@scientech.com)

18. Fwd: ms02-018 IS dangerous after all (Thread)

Relevant URL:

[200204172204.g3HM4vY31459@mailserver4.hushmail.com">http://online.securityfocus.com/archive/88/2002041722](http://online.securityfocus.com/archive/88/200204172204.g3HM4vY31459@mailserver4.hushmail.com)

19. SSL directory structure issue (Thread)

Relevant URL:

[E846E1497BC9E747A88011167C797D0A09B3AC@pantera.corp.workscape.net">http://online.securityfocus.com/ar](http://online.securityfocus.com/arE846E1497BC9E747A88011167C797D0A09B3AC@pantera.corp.workscape.net)

20. Any known issue with 10 April 2002 Cumulative Patch for IIS ? (Thread)

Relevant URL:

<http://online.securityfocus.com/archive/88/5.1.0.14.0.20020416124636.0323d138@192.168.3.190>

21. Any known issue with 10 April 2002 Cumulative Patch for IIS ? (Thread)

Relevant URL:

[Pine.BSF.4.21.0204161153470.53719-100000@ns1.inlinenet.net">http://online.securityfocus.com/archive/88/Pine.BS](http://online.securityfocus.com/archive/88/Pine.BSF.4.21.0204161153470.53719-100000@ns1.inlinenet.net)

SecurityFocus Microsoft: SecurityFocus Microsoft Newsletter #83

22. Administrivia: Users slam Microsoft Security Analyser (Thread)

Relevant URL:

[Pine.LNX.4.43.0204161036420.10444-100000@mail.securityfocus.com](http://online.securityfocus.com/archive/88/Pine.LNX.4.43.0204161036420.10444-100000@mail.securityfocus.com)">http://online.securityfocus.com/archive/88/

23. SSL directory structure issue (Thread)

Relevant URL:

[20020416160923.83021.qmail@web14909.mail.yahoo.com](http://online.securityfocus.com/archive/88/20020416160923.83021.qmail@web14909.mail.yahoo.com)">http://online.securityfocus.com/archive/88/20020416160

24. Posters Slam Microsoft Training (Thread)

Relevant URL:

[7FE1FAD6701BD21180ED0001FAD464A9033CE607@sw820x033.visa.com](http://online.securityfocus.com/archi7FE1FAD6701BD21180ED0001FAD464A9033CE607@sw820x033.visa.com)">http://online.securityfocus.com/archi

25. Users slam Microsoft Security Analyser (Thread)

Relevant URL:

[E00ECDED326C0B4288A0B4F7F02DE2DD131A5F@mickey.questinc.org](http://online.securityfocus.com/archivE00ECDED326C0B4288A0B4F7F02DE2DD131A5F@mickey.questinc.org)">http://online.securityfocus.com/archiv

26. Users slam Microsoft Security Analyser (Thread)

Relevant URL:

[http://online.securityfocus.com/archive/88/003b01c1e4db\\$b6ca5a50\\$0800a8c0@VAIO](http://online.securityfocus.com/archive/88/003b01c1e4db$b6ca5a50$0800a8c0@VAIO)

27. SecurityFocus Microsoft Newsletter #82 (Thread)

Relevant URL:

[Pine.LNX.4.43.0204151549500.4056-100000@mail.securityfocus.com](http://online.securityfocus.com/archive/88/Pine.LNX.4.43.0204151549500.4056-100000@mail.securityfocus.com)">http://online.securityfocus.com/archive/88/P

28. Posters Slam Microsoft Training (Thread)

Relevant URL:

[6e00010a@lauradominion.com](http://online.securityfocus.com/archive/88/005c01c1e4c5$d8aea920$6e00010a@laur6e00010a@lauradominion.com)">http://online.securityfocus.com/archive/88/005c01c1e4c5\$d8aea920\$6e00010a@laur

29. URLSCAN error 50 (Thread)

Relevant URL:

[20020415202639.19901.qmail@mail.securityfocus.com](http://online.securityfocus.com/archive/88/20020415202639.19901.qmail@mail.securityfocus.com)">http://online.securityfocus.com/archive/88/20020415202639

30. Scanning MS DHCP networks. Reading dhcp.mdb (Thread)

Relevant URL:

[F3CFDEEC7F81D311AA7B0090279AA2F4FAC822@sdefusr1.france.ppg.com](http://online.securityfocus.com/archF3CFDEEC7F81D311AA7B0090279AA2F4FAC822@sdefusr1.france.ppg.com)">http://online.securityfocus.com/arch

31. Scanning MS DHCP networks. Reading dhcp.mdb (Thread)

Relevant URL:

[http://online.securityfocus.com/archive/88/00cc01c1e49b\\$7e3b64d0\\$01f9a8c0@localdomain](http://online.securityfocus.com/archive/88/00cc01c1e49b$7e3b64d0$01f9a8c0@localdomain)

32. Anyone familiar with bitvise's winsshd? (Thread)

Relevant URL:

[NFBBKIJOMENLOPEIOHLMGELLCDAAMaarten@UnitedConsumers.com">http://online.securityfocus.com/archi](http://online.securityfocus.com/archi)

33. VPN / IPSEC (Thread)

Relevant URL:

34. Peculiar login troubles. (Thread)

Relevant URL:

[http://online.securityfocus.com/archive/88/002701c1e455\\$e35d9a40\\$0a01a8c0@slelaptop](http://online.securityfocus.com/archive/88/002701c1e455$e35d9a40$0a01a8c0@slelaptop)

35. authentication NTLM (Thread)

Relevant URL:

[AMEMLFHFFINNIIBIBAAODAEBGDCAA.alicia.laing@verizon.net">http://online.securityfocus.com/archive/88/AM](http://online.securityfocus.com/archive/88/AM)

IV. NEW PRODUCTS FOR MICROSOFT PLATFORMS

1. Datakey CIP

by Datakey

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

Relevant URL:

<http://www.datakey.com/CIP/index.html>

Summary:

Datakey CIP is Datakey's complete cryptographic smart card and interface software package for government agencies, financial institutions and enterprises, enabling enhanced security and strong user authentication for business-to-business e-commerce. CIP seamlessly integrates and interoperates with solutions from today's leading information security vendors, including VPNs, extranets and PKI-ready applications or environments. The CIP suite – featuring Datakey's Model 330 smart card – allows users to securely store and use their digital credentials, adds two-factor security to environments that require secure authentication, and provides the added convenience of digital cred