

SecurityFocus Microsoft Newsletter #84

Source: <http://www.derkeiler.com/Mailing-Lists/securityfocus/focus-ms/2002-04/0332.html>

From: Marc Fossi (mfossi@securityfocus.com)

Date: 04/29/02

Date: Mon, 29 Apr 2002 15:16:32 -0600 (MDT)
From: Marc Fossi <mfossi@securityfocus.com>
To: Focus-MS <focus-ms@securityfocus.com>

SecurityFocus Microsoft Newsletter #84

This issue is sponsored by: Citadel Security Software

The most critical piece of vulnerability assessment is remediation. Now that you're scanning for those vulnerabilities, how are you going to repair them all? Hercules, from Citadel Security Software, automates the remediation process from a single point of control saving as much as 80% of the time it takes to secure your network. You simply select which repairs you wish to automate and Hercules takes care of the rest.

Download a free trial version of Hercules today at <http://www.citadel.com/hercules.asp> or call 1-888-5CITADEL (1-888-524-8233) for more information.

I. FRONT AND CENTER

1. Securing Privacy, Part Two: Software Issues
2. Securing Exchange 2000
3. Teaching the Rules of the Road
4. Dollar Diddling and the Billion Dollar Viruses

II. MICROSOFT VULNERABILITY SUMMARY

1. Macromedia Flash ActiveX Control Bandwidth Consumption...
2. Microsoft IIS CodeBrws.ASP File Extension Check Out By One...
3. PVote Poll Content Manipulation Vulnerability
4. IcrediBB Script Injection Vulnerability
5. Foundstone FScan Banner Grabbing Format String Vulnerability
6. WorkforceROI XPede Unprotected Administrative Facilities...
7. XPede DataSource.ASP Information Disclosure Vulnerability
8. WorkforceROI XPede Weak File Protection Vulnerability
9. WorkforceROI XPede Sprc.ASP SQL Injection Vulnerability...
10. Snitz Forums 2000 Members.ASP SQL Injection Vulnerability
11. vqServer CGI Demo Program Script Injection Vulnerability
12. PVote Unauthorized Administrative Password Change Vulnerability

13. Philip Chinery's Guestbook Script Injection Vulnerability
14. Matu FTP Client Buffer Overflow Vulnerability
15. ColdFusion DOS Device File Request System Information...
17. WorkforceROI XPede Arbitrary Time Sheet Disclosure Vulnerability
18. Microsoft Internet Explorer Self-Referential Object Denial...
19. Apache Tomcat Servlet Path Disclosure Vulnerability
20. National Instruments LabVIEW HTTP Request Denial of Service...
21. Internet Explorer Recursive JavaScript Event Denial of Service...
22. Microsoft Outlook Express DOS Device Denial of Service...

III. MICROSOFT FOCUS LIST SUMMARY

1. Remote perf counter access (Thread)
2. problems with hotfix rollup, windows update, mbsa, hfnetchk...
3. Network Settings and Power Users (Thread)
4. Update on status of IE security (Thread)
5. Question: How To Secure a Public Access Workstation (Thread)
6. Microsoft Cluster in DMZ – Need Advice (Thread)
7. MS defends MBSA (Thread)
8. Network Settings and Power Users (Thread)
9. problems with hotfix rollup, windows update, mbsa, hfnetchk...
10. Remote perf counter access (Thread)
11. Role based access in Win2k w/o AD (Thread)
12. Follow-up on Registry key containing events to be audited
13. MS defends MBSA (Thread)
14. IE 5.5 security (Thread)
15. Securing IIS (Thread)
16. SecurityFocus Microsoft Newsletter #83 (Thread)
17. Securing IIS (Thread)
18. Registry keys for EventLog audit events (Thread)
19. Question: How To Secure a Public Access Workstation (Thread)
20. HFNetCheck Pro in an NT-only environment? (Thread)
21. Microsoft Cluster in DMZ – Need Advice (Thread)
22. windows domain question (Thread)
23. windows domain question (Thread)
24. OWA and URLScan (Thread)
25. URLScan 2.5 SRP (Thread)
26. Microsoft Security Bulletin MS01-022 (Thread)
27. Ensuring Disabling/Uninstallation of Windows XP Firewall in...
28. OWA and URLScan (Thread)
29. Ensuring Disabling/Uninstallation of Windows XP Firewall in...
30. Win 98 Security (Thread)
31. Microsoft Security Bulletin MS01-022 (Thread)
32. Win 98 Security (Thread)
33. Ensuring Disabling/Uninstallation of Windows XP Firewall in LAN...

IV. NEW PRODUCTS FOR MICROSOFT PLATFORMS

1. iSpyNOW
2. ipPulse
3. Netsecure Mail

V. NEW TOOLS FOR MICROSOFT PLATFORMS

1. EGADS v0.9
2. DSCMD – DataSAFE Command Line Encryptor v2.0
3. Cain & Abel v2.5beta11

4. Bouncer v1.0.RC6

VI. SPONSORSHIP INFORMATION

I. FRONT AND CENTER

1. Securing Privacy, Part Two: Software Issues

By Scott Granneman

This is the second article in a three-part series that will examine privacy concerns as they relate to security. This installment will discuss software-based issues and solutions. As we shall see, some software is designed to safeguard privacy, while other software seems designed to compromise it.

<http://online.securityfocus.com/infocus/1573>

2. Securing Exchange 2000

by Chris Weber

This article is the first of a two-part series that will provide a technical look at some of the fundamental requirements for securing Microsoft Exchange Server 2000 and Outlook Web Access (OWA) running in a Windows 2000 Active Directory environment. I will start by looking at some exploits for Exchange server to give readers an idea of areas that need protection. Then I'll get right into the Exchange application and discuss some of its inherent security features, as well as some secure network designs for Exchange/OWA deployments.

<http://online.securityfocus.com/infocus/1572>

3. Teaching the Rules of the Road

By Jon Lasser

Bad system administrators affect more than their own computers -- they make the entire Internet a little less safe.

<http://online.securityfocus.com/columnists/77>

4. Dollar Diddling and the Billion-Dollar Viruses

By George Smith

How journalists tap "experts" to reach absurd conclusions about the cost of computer viruses.

<http://online.securityfocus.com/columnists/78>

II. BUGTRAQ SUMMARY

1. Macromedia Flash ActiveX Control Bandwidth Consumption Vulnerability

BugTraq ID: 4567

Remote: Yes

Date Published: Apr 19 2002 12:00A

Relevant URL:

<http://www.securityfocus.com/bid/4567>

Summary:

The Macromedia Flash Player is available as an ActiveX plugin for Microsoft Internet Explorer. An issue in version 6 of this component may result in excessive bandwidth consumption.

Under normal usage, the Flash Player must download a variety of multimedia resources, including video, sound and image files. Under some circumstances, the user may navigate to a different page before this process is complete. In this case, it is possible that the player will continue to download outdated information, consuming unnecessary bandwidth. As these files can be large, this may result in a denial of service condition.

Macromedia has reported that only the ActiveX version of the Flash Player suffers from this vulnerability.

2. 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.

3. 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.

4. 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.

5. 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 a free 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.

6. 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.

7. 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.

8. 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.

9. 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.

10. 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.

11. vqServer CGI Demo Program Script Injection Vulnerability

BugTraq ID: 4573

Remote: Yes

Date Published: Apr 21 2002 12:00A

Relevant URL:

<http://www.securityfocus.com/bid/4573>

Summary:

vqServer is a HTTP server implemented in Java. vqServer is available on any architecture supporting Java, including Linux and Microsoft Windows.

vqServer supports a variety of CGI mechanisms, including Perl scripts, executables and servlets. vqServer includes a number of demonstration programs for these methods.

Issues have been reported with multiple scripts included with vqServer. Reportedly, it is possible to inject JavaScript code through these programs. In addition to cross site scripting issues, it has been reported possible to inject script code into cookie content.

Exploitation of these sample programs may allow an attacker to execute script code in the context of the page hosted with vqServer.

12. 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.

13. Philip Chinery's Guestbook Script Injection Vulnerability

BugTraq ID: 4566

Remote: Yes

Date Published: Apr 21 2002 12:00A

Relevant URL:

<http://www.securityfocus.com/bid/4566>

Summary:

Philip Chinery's Guestbook is freely available guestbook software. It will run on most Unix and Linux variants, as well as Microsoft Windows operating systems.

Philip Chinery's Guestbook does not filter HTML tags from form fields. As a result, it is possible for an attacker to inject script code into pages that are generated by the guestbook. Additionally, script code is not filtered from URL parameters, making the guestbook prone to cross-site scripting attacks.

In both instances, it is possible for an attacker to cause arbitrary script code to be executed in the browser of a web user, in the security context of the website running the vulnerable guestbook.

This may allow the attacker to hijack web content or potentially steal cookie-based authentication credentials.

This issue has been reported for Philip Chinery's Guestbook version 1.1. Other versions may also be affected.

14. Matu FTP Client Buffer Overflow Vulnerability

BugTraq ID: 4572

Remote: Yes

Date Published: Apr 23 2002 12:00A

Relevant URL:

<http://www.securityfocus.com/bid/4572>

Summary:

Matu FTP is an ftp client that runs on various Microsoft Windows operating systems.

An issue has been reported which could allow for a malicious ftp host to execute arbitrary code on a Matu FTP client.

This is achievable when a Matu FTP user connects to an ftp host, if the FTP server '220' response is of excessive length. A stack-based overflow condition can occur, potentially allowing for malicious administrators to execute arbitrary code on (and gain control of) client hosts. However, sending random data could cause the application to crash.

15. 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.

16. Multiple Stack Protection Scheme Function Argument Overwrite Weakness

BugTraq ID: 4586

Remote: Yes

Date Published: Apr 24 2002 12:00A

Relevant URL:

<http://www.securityfocus.com/bid/4586>

Summary:

Multiple application-layer technologies exist to prevent exploitation of stack-overflow conditions. A paper describing a number of new weaknesses in these technologies has been recently published.

The weakness described in this report is a lack of protection of function parameters. Affected by this weakness are programs compiled with StackGuard, StackShield, and the Microsoft Visual C++ .NET /GS option.

When a stack overflow occurs, it is often possible for the attacker to overwrite data beyond the procedure activation record. In typical Intel C programs, the data pushed on the stack before the return address when a procedure is invoked is that comprising its arguments. An attacker is often able to corrupt procedure arguments due to their proximity on the stack. Under specific circumstances, this may result in the ability to write almost anywhere in memory.

There is no practical way for a procedure to determine, while it is executing, if the arguments have been corrupted or not. A circumstance may occur where a pointer that was passed to the function is used as the destination address in a memory write operation after a stack overflow condition. In this situation, the attacker can exploit the overflow condition prior to the memory write so that a target address replaces the pointer argument. When the memory write occurs, data will be written to an attacker-specified location.

The exploitation attempt, having overwritten the local variables and activation record, would trigger StackGuard's/Microsoft's Visual Studio .NET /GS protection mechanism. Unfortunately, StackGuard uses library procedures before terminating the process. An attacker exploiting this

weakness would have the ability to write data anywhere, including over the GOT entries for these library functions. It is assumed that the Microsoft /GS protection handler calls functions by reference as well. If this is the case, the feature may be evaded using a similar technique.

Programs protected with StackShield will continue to run, as the protection does not involve verifying the integrity of the stack frame. The attacker would be required to replace GOT entries for procedures called after the function returned. If this does not occur in the lifetime of the process, the condition cannot be successfully exploited.

17. 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.

18. Microsoft Internet Explorer Self-Referential Object Denial of Service Vulnerability

BugTraq ID: 4564

Remote: Yes

Date Published: Apr 20 2002 12:00A

Relevant URL:

<http://www.securityfocus.com/bid/4564>

Summary:

Microsoft Internet Explorer 6 (perhaps other versions as well) is vulnerable to a denial of service due to an error in handling certain self-referential <OBJECT> definitions in HTML documents. This occurs when an object of type "text/html" is specified, with the DATA field referencing the name of the HTML document in which it is defined. There may be other circumstances in which this sort of self-reference may lead to a browser crash.

19. Apache Tomcat Servlet Path Disclosure Vulnerability

BugTraq ID: 4575

Remote: Yes

Date Published: Apr 23 2002 12:00A

Relevant URL:

<http://www.securityfocus.com/bid/4575>

Summary:

Apache Tomcat is a servlet container for use with the Java Servlet and JavaServer Pages technologies. Tomcat may be run on most Unix and Linux variants as well as Microsoft Windows operating systems.

A problem in the default installation of Apache Tomcat may cause sensitive information to be disclosed to remote attackers.

Apache Tomcat ships with a number of example classes (SnoopServlet and TroubleShooter) which may reveal the absolute path of the Tomcat installation when requested via HTTP. These classes are included to serve as an example for developers and are not intended to be used in production environments.

This information will give the attacker an idea of the layout of the filesystem on the host running Apache Tomcat. Disclosure of this type of sensitive information may aid in further attacks against the host running the vulnerable software.

20. National Instruments LabVIEW HTTP Request Denial of Service Vulnerability

BugTraq ID: 4577

Remote: Yes

Date Published: Apr 19 2002 12:00A

Relevant URL:

<http://www.securityfocus.com/bid/4577>

Summary:

A vulnerability has been reported in some versions of National Instruments LabVIEW for Linux and Microsoft Windows.

LabVIEW includes an integrated HTTP server. If a malformed HTTP request is received, it is possible to crash the LabVIEW Web Server and LabVIEW itself. This condition occurs when an HTTP GET request is received and terminated with two new line characters, as opposed to the compliant carriage return / new line combination.

Exploitation of this vulnerability may result in a denial of service condition. It is not currently known if exploitation will allow the execution of arbitrary code as the server process.

It has been reported that this vulnerability may only be exploited if logging is enabled on the web server.

21. Internet Explorer Recursive JavaScript Event Denial of Service Vulnerability

BugTraq ID: 4583

Remote: Yes

Date Published: Apr 24 2002 12:00A

Relevant URL:

<http://www.securityfocus.com/bid/4583>

Summary:

An issue has been reported in some versions of Microsoft Internet Explorer. It is possible for a malicious web page using JavaScript to crash the browser process. Under some environments, this may impact the underlying operating system as well.

This behavior has been reported under the following circumstances. An IMG tag is created with an invalid SRC attribute, and a malicious script is defined using the onError parameter for the tag. This script, in turn, resets the SRC attribute to the same value. The result is an indirect recursive call of the script, which is able to consume all available stack memory.

It is possible that other conditions will exploit this vulnerability. This has not, however, been confirmed.

Under these conditions, Internet Explorer has been reported to crash. Under Windows 95 and 98 this has been reported to cause instability in the operating system. More recent versions of Windows have been reported to be unaffected.

22. Microsoft Outlook Express DOS Device Denial of Service Vulnerability

BugTraq ID: 4584

Remote: Yes

Date Published: Apr 24 2002 12:00A

Relevant URL:

<http://www.securityfocus.com/bid/4584>

Summary:

A denial of service issue has been reported in Microsoft Outlook Express.

Reportedly, this issue occurs if an HTML email message with a URL pointing to a non-existent DOS-device (CON, AUX, PRN, NUL), is embedded in the BGSOUND or IFRAME tag. Upon the user opening the mail message, Outlook Express will consume 100% CPU usage.

Either the process is ended via the Task Manager or a system restart is required in order to regain normal functionality.

It has also been reported that the offending message cannot be deleted from the user's mailbox. If this is the case, re-installation of Outlook Express may be required.

This issue may be the result of an unchecked buffer. If this is the case, there is a possibility that arbitrary code may be executed on the vulnerable target. However, this has not yet been confirmed.

III. MICROSOFT FOCUS LIST SUMMARY

1. Remote perf counter access (Thread)

Relevant URL:

<http://online.securityfocus.com/archive/88/D9CC6F05BDF4D211B6EF00508BAD0786021D1926@SRVNT-TVW09>

2. problems with hotfix rollup, windows update, mbsa, hfnetchk, and (Thread)

Relevant URL:

[OF10780DB0.F8B88425-ON85256BA6.0067A6AB@sbcs.com](http://online.securityfocus.com/archive/88/OF10780DB0.F8B88425-ON85256BA6.0067A6AB@sbcs.com)"><http://online.securityfocus.com/archive/88/OF10780DB0.F8B88425-ON85256BA6.0067A6AB@sbcs.com>

3. Network Settings and Power Users (Thread)

Relevant URL:

[7771AA69152BD61197E700B0D0D1B725867F08@exchange106.comp.pge.com](http://online.securityfocus.com/archive/88/7771AA69152BD61197E700B0D0D1B725867F08@exchange106.comp.pge.com)"><http://online.securityfocus.com/archive/88/7771AA69152BD61197E700B0D0D1B725867F08@exchange106.comp.pge.com>

4. Update on status of IE security (Thread)

Relevant URL:

[B8ED98E8.92B%ben@jatomail.net](http://online.securityfocus.com/archive/88/B8ED98E8.92B%ben@jatomail.net)"><http://online.securityfocus.com/archive/88/B8ED98E8.92B%ben@jatomail.net>

5. Question: How To Secure a Public Access Workstation (Thread)

Relevant URL:

[OF0C500132.D47ACA22-ON85256BA6.0053F055@bna.com](http://online.securityfocus.com/archive/88/OF0C500132.D47ACA22-ON85256BA6.0053F055@bna.com)"><http://online.securityfocus.com/archive/88/OF0C500132.D47ACA22-ON85256BA6.0053F055@bna.com>

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

Relevant URL:

[http://online.securityfocus.com/archive/88/000e01c1ec6f\\$fee2b580\\$caf4450a@deth](http://online.securityfocus.com/archive/88/000e01c1ec6f$fee2b580$caf4450a@deth)

7. MS defends MBSA (Thread)

Relevant URL:

[6D9F17809993D31198B100508B62016106F46B09@nt-exchange.ifas.ufl.edu](http://online.securityfocus.com/archive/88/6D9F17809993D31198B100508B62016106F46B09@nt-exchange.ifas.ufl.edu)"><http://online.securityfocus.com/archive/88/6D9F17809993D31198B100508B62016106F46B09@nt-exchange.ifas.ufl.edu>

8. Network Settings and Power Users (Thread)

Relevant URL:

[3CC7E7E8.8C8B8A8@agcs.com](http://online.securityfocus.com/archive/88/3CC7E7E8.8C8B8A8@agcs.com)"><http://online.securityfocus.com/archive/88/3CC7E7E8.8C8B8A8@agcs.com>

9. problems with hotfix rollup, windows update, mbsa, hfnetchk, and other tools (Thread)

Relevant URL:

[20020425021004.25104.qmail@mail.securityfocus.com](http://online.securityfocus.com/archive/88/20020425021004.25104.qmail@mail.securityfocus.com)"><http://online.securityfocus.com/archive/88/20020425021004.25104.qmail@mail.securityfocus.com>

SecurityFocus Microsoft: SecurityFocus Microsoft Newsletter #84

10. Remote perf counter access (Thread)

Relevant URL:

<http://online.securityfocus.com/archive/88/1019698417.1441.9.camel@spectre>

11. Role based access in Win2k w/o AD (Thread)

Relevant URL:

[77F055FA968580429F4546414D8C10E705E2DB@s102.rhcci.com](http://online.securityfocus.com/archive/88/77F055FA968580429F4546414D8C10E705E2DB@s102.rhcci.com)"><http://online.securityfocus.com/archive/88/77F055FA968580429F4546414D8C10E705E2DB@s102.rhcci.com>

12. Follow-up on Registry key containing events to be audited (Thread)

Relevant URL:

[20020424123340.58910.qmail@web20505.mail.yahoo.com](http://online.securityfocus.com/archive/88/20020424123340.58910.qmail@web20505.mail.yahoo.com)"><http://online.securityfocus.com/archive/88/20020424123340.58910.qmail@web20505.mail.yahoo.com>

13. MS defends MBSA (Thread)

Relevant URL:

[20020424082410.6932836F9@sitemail.everyone.net](http://online.securityfocus.com/archive/88/20020424082410.6932836F9@sitemail.everyone.net)"><http://online.securityfocus.com/archive/88/20020424082410.6932836F9@sitemail.everyone.net>

14. IE 5.5 security (Thread)

Relevant URL:

[200204240031.g3O0VS253742@mailserver2.hushmail.com](http://online.securityfocus.com/archive/88/200204240031.g3O0VS253742@mailserver2.hushmail.com)"><http://online.securityfocus.com/archive/88/200204240031.g3O0VS253742@mailserver2.hushmail.com>

15. Securing IIS (Thread)

Relevant URL:

[20020423050259.16294.qmail@reznor.com](http://online.securityfocus.com/archive/88/20020423050259.16294.qmail@reznor.com)"><http://online.securityfocus.com/archive/88/20020423050259.16294.qmail@reznor.com>

16. SecurityFocus Microsoft Newsletter #83 (Thread)

Relevant URL:

[Pine.LNX.4.43.0204221500590.5962-100000@mail.securityfocus.com](http://online.securityfocus.com/archive/88/Pine.LNX.4.43.0204221500590.5962-100000@mail.securityfocus.com)"><http://online.securityfocus.com/archive/88/Pine.LNX.4.43.0204221500590.5962-100000@mail.securityfocus.com>

17. Securing IIS (Thread)

Relevant URL:

[8EC06C4282C97848B85CA4C23906991101156047@ntx1.forest.netvision.net.il](http://online.securityfocus.com/archive/88/8EC06C4282C97848B85CA4C23906991101156047@ntx1.forest.netvision.net.il)"><http://online.securityfocus.com/archive/88/8EC06C4282C97848B85CA4C23906991101156047@ntx1.forest.netvision.net.il>

18. Registry keys for EventLog audit events (Thread)

Relevant URL:

<http://online.securityfocus.com/archive/88/3CC457ED.14103.362F46@localhost>

19. Question: How To Secure a Public Access Workstation (Thread)

Relevant URL:

[D5E5F4682E75D41185CD00D0B79DC56F04BB1AC5@exchfed01.federatedinv.com](http://online.securityfocus.com/archive/88/D5E5F4682E75D41185CD00D0B79DC56F04BB1AC5@exchfed01.federatedinv.com)"><http://online.securityfocus.com/archive/88/D5E5F4682E75D41185CD00D0B79DC56F04BB1AC5@exchfed01.federatedinv.com>

SecurityFocus Microsoft: SecurityFocus Microsoft Newsletter #84

20. HFNetCheck Pro in an NT-only environment? (Thread)

Relevant URL:

<http://online.securityfocus.com/archive/88/3CC40406.8885.10E21A8@localhost>

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

Relevant URL:

[caf4450a@ndpms.org">http://online.securityfocus.com/archive/88/023001c1e88a\\$c0b7b3c0\\$caf4450a@ndpms.org](http://online.securityfocus.com/archive/88/023001c1e88a$c0b7b3c0$caf4450a@ndpms.org)

22. windows domain question (Thread)

Relevant URL:

<http://online.securityfocus.com/archive/88/1019278924.1590.37.camel@FranksLaptop>

23. windows domain question (Thread)

Relevant URL:

[6e00010a@lauradominion.com">http://online.securityfocus.com/archive/88/16f901c1e7e7\\$d3965170\\$6e00010a@lauradominion.com](http://online.securityfocus.com/archive/88/16f901c1e7e7$d3965170$6e00010a@lauradominion.com)

24. 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)

25. 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)

26. 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)

27. Ensuring Disabling/Uninstalation 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)

28. OWA and URLScan (Thread)

Relevant URL:

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

29. Ensuring Disabling/Uninstalation 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)

30. Win 98 Security (Thread)

Relevant URL:

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

31. Microsoft Security Bulletin MS01-022 (Thread)

Relevant URL:

[3CC0279E.CE5F5D2C@espgroup.net">http://online.securityfocus.com/archive/88/3CC0279E.CE5F5D2C@espgroup.net](http://online.securityfocus.com/archive/88/3CC0279E.CE5F5D2C@espgroup.net)

32. Win 98 Security (Thread)

Relevant URL:

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

33. 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)

IV. NEW PRODUCTS FOR MICROSOFT PLATFORMS

1. iSpyNOW

by Spy Software Solutions

Platforms:

Relevant URL:

<http://www.spy-software-solutions.com/ispy.htm>

Summary:

iSpyNOW is a remote install spy software product. Remotely monitor computers without the need of having to physically access or install software. iSpyNOW offers you the ability to remotely install the spy software from any location and via the logs from anywhere in the world.

2. ipPulse

by Northwest Performance Software

Platforms: Windows 95/98, Windows NT

Relevant URL:

<http://www.ippulse.com/ippulsemain.html>

Summary:

ipPulse is a Remote Status Monitoring Tool. Use ipPulse to monitor the up/down status of IP connected devices (nodes) on any IP connected network. ipPulse uses a variety of methods, including SNMP, to poll and check the network connectivity of a list of user-defined nodes. ipPulse alerts you to failures using a variety of techniques ranging from audible messages to email and pager notification. You can even control ipPulse remotely by logging into Remote Control using any Telnet application.

3. Netsecure Mail

by NetSecure Software

Platforms: Java, Windows NT

Relevant URL:

http://www.netsecuresoftware.com/netsecurenew/Products/NetSecure_Mail/netsecure_mail.html

Summary:

With NetSecure Mail, you can provide Email service to your users while ensuring that your information system is protected and separate from the Internet. The NetSecure Mail architecture allows you to: * Receive Emails through Internet in a separate area called the DeMilitarized Zone (DMZ) * Eradicate viruses received Emails with a specialized anti-virus tool in the DMZ * Retrieve Emails stored in your DMZ from your LAN using NetSecure Mail. Email is forwarded to your LAN Mail Server as it arrives through the Internet.

V. NEW TOOLS FOR MICROSOFT PLATFORMS

1. EGADS v0.9

by Secure Software Solutions

Relevant URL:

<http://www.securesw.com/egads/>

Platforms: UNIX, Windows 2000

Summary:

EGADS is a system service and library for providing secure random numbers. It contains an implementation of the Tiny pseudo-random number generator and the Tiny entropy gateway. Tiny is an evolution of Yarrow, and was designed by John Kelsey (an original designer of Yarrow) and John Viega. We are currently preparing a white paper on the Tiny algorithm.

EGADS provides the same kind of functionality as /dev/random and /dev/urandom on Linux systems, but works on Windows, and as a portable Unix program.

EGADS is available as a portable user-level daemon for Unix systems, and as a service for Windows 2000 machines. An XP-compatible version will be available shortly.

2. DSCMD – DataSAFE Command Line Encryptor v2.0

by Regnoc Software

Relevant URL:

<http://www.regnoc.com>

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

Summary:

DSCMD allows you to encrypt source files for secure storage, transmission via the Internet, and e-mail attachments. Only someone who knows the eight-character locking combination can recover the contents of the encrypted file. DSCMD is completely command-line driven, and simple to integrate into your programs and scripts on both Windows NT and Linux servers.

3. Cain & Abel v2.5beta11

by mao

Relevant URL:

<http://www.oxid.it>

Platforms: Windows 95/98

Summary:

Cain is a password recovery tool for Windows 95/98 operating systems. It allows easy recovery of Logon passwords, Share passwords (local and remote), Screen Saver passwords, Access Database passwords, DialUp passwords, Link passwords and any other application defined password cached in your system or in external .PWL and registry files. SMB passwords (MD4 hashed passwords) can also be recovered with a powerful distributed SMB sniffer.

4. Bouncer v1.0.RC6

by Chris Mason chris@r00t3d.org.uk

Relevant URL:

<http://www.r00t3d.org.uk/bin/>

Platforms: FreeBSD, Linux, OpenBSD, Solaris, Windows 2000, Windows NT

Summary:

Bouncer is a network tool which allows you to bypass proxy restrictions and obtain outside connections from an internal LAN. It uses SSL tunneling, which allows you to obtain a constant streaming connection out of a proxy. If you are restricted behind a proxy and can access secure online ordering sites, then you can get out to whatever host on whatever port you want. It also supports a lot of other features including socks 5, basic authentication, access control lists, and Web-based administration, and will run on Windows, Linux, and FreeBSD.

VI. SPONSORSHIP INFORMATION

This issue is sponsored by: Citadel Security Software

The most critical piece of vulnerability assessment is remediation. Now that you're scanning for those vulnerabilities, how are you going to repair them all? Hercules, from Citadel Security Software, automates the remediation process from a single point of control saving as much as 80% of the time it takes to secure your network. You simply select which repairs you wish to automate and Hercules takes care of the rest.

Download a free trial version of Hercules today at

<http://www.citadel.com/hercules.asp> or call 1-888-5CITADEL

(1-888-524-8233) for more information.

-
- **Previous message:** [Mike Coppins: "Re: Account Permissions"](#)
 - **Messages sorted by:** [\[date \]](#) [\[thread \]](#) [\[subject \]](#) [\[author \]](#) [\[attachment \]](#)