

SecurityFocus Microsoft Newsletter #140

Source: <http://www.derkeiler.com/Mailing-Lists/securityfocus/focus-ms/2003-06/0003.html>

From: Marc Fossi (*mfossi_at_securityfocus.com*)

Date: 06/09/03

Date: Mon, 9 Jun 2003 11:41:03 -0600 (MDT)

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

SecurityFocus Microsoft Newsletter #140

This issue brought to you by: SPI Dynamics

FREE White Paper: "How A Hacker Launches A Web Application Attack!"

Learn why 70% of today's successful hacks involve Web Application attacks such as: SQL Injection, XSS, Cookie Manipulation, and Parameter Manipulation. All undetectable by Firewalls and IDS! Download *FREE* white paper from SPI Dynamics for a complete guide to protection!

<http://www.securityfocus.com/SPIDynamics-ms-secnews2>

I. FRONT AND CENTER

1. The Enemy Within: Firewalls and Backdoors
2. Adding Security to the Cert
3. Learning to Love Big Brother
4. Welcome to the SecurityFocus Firewalls Focus Area
5. Welcome to the SecurityFocus Pen-Test Focus Area

II. MICROSOFT VULNERABILITY SUMMARY

1. Cafelog b2 Remote File Include Vulnerability
2. Webroot Shoutbox Remote Command Execution Vulnerability
3. myServer HTTP GET Argument Buffer Overflow Vulnerability
4. Cafelog b2 B2MenuTop Script B2INC Variable Include Vulnerability
5. Geeklog Image Upload Extension Validation Vulnerability
6. Activity Monitor 2002 Remote Denial of Service Vulnerability
7. Pablo Software Solutions Baby POP3 Server Multiple Connection...
8. Microsoft Internet Explorer False URL Information Vulnerability
9. WebCortex WebStores2000 SQL Injection Vulnerability
10. Gator EWallet Information Encoding Weakness
11. Microsoft Windows 2000/XP/2003 IPV6 ICMP Flood Denial Of...
12. Microsoft Windows XP Nested Directory Denial of Service...
13. IRCXpro Server Settings.INI Plaintext Password Storage...

14. Pablo Software Solutions FTP Server Anonymous Users...
15. Pablo Software Solutions FTP Server Plaintext Password Weakness
16. Webfroot Shoutbox URI Parameter File Disclosure Vulnerability
17. FrontRange Solutions GoldMine HTML Mail Script Execution...
18. Geeklog Authentication SQL Injection Vulnerability
19. Pablo Software Solutions Baby FTP Server Directory Traversal...
20. Pablo Software Solutions Baby FTP Server Multiple Connection...
21. Pablo Software Solutions Baby Web Server Multiple Connection...
22. Pablo Software Solutions Quick and Easy FTP Server Denial Of...
23. Pablo Software Solutions Baby Web Server Directory Traversal...
24. Desktop Orbiter Resource Exhaustion Denial Of Service...
25. PHP Transparent Session ID Cross Site Scripting Vulnerability
26. iisCart2000 Arbitrary File Upload Vulnerability
27. Microsoft URLScan Information Disclosure Weakness
28. WinMX Plaintext Password Storage Weakness
29. Webfroot Shoutbox Expanded.PHP Remote Command Execution...
30. Webfroot Shoutbox Expanded.PHP Remote Directory Traversal...
31. Cafelog b2 B2Functions Script B2INC Variable Include...
32. CafeLog b2 Blog.Header Script SQL Injection Vulnerability
33. Pi3Web SortName Buffer Overflow Vulnerability

III. MICROSOFT FOCUS LIST SUMMARY

1. Announcement: SecurityFocus Pen-Test and Firewalls...
2. SecurityFocus Microsoft Newsletter #139 (Thread)
3. Internet Explorer URL Spoofing Threat (Thread)

IV. NEW PRODUCTS FOR MICROSOFT PLATFORMS

1. OrangeBox Mail
2. Restorer2000 Data Recovery Software
3. CyProtect File Encryption

V. NEW TOOLS FOR MICROSOFT PLATFORMS

1. LibTomCrypt v0.76
2. A Joint Monitoring System (AJMS) v1.8
3. Gherkin v0.2.2

VI. SPONSOR INFORMATION

I. FRONT AND CENTER

1. The Enemy Within: Firewalls and Backdoors
by Bob Rudis, CISSP, and Phil Kostenbade, CISSP

This article presents an overview of modern backdoor techniques, discusses how they can be used to bypass the security infrastructure that exists in most network deployments and issues a wake-up call for those relying on current technologies to safeguard their systems/networks.

<http://www.securityfocus.com/infocus/1701>

2. Adding Security to the Cert
By Tim Mullen

Shiftless third-party prep courses have made MCSE certification less valuable. Is Microsoft's new security cert doomed to the same fate?

<http://www.securityfocus.com/columnists/166>

3. Welcome to the SecurityFocus Firewalls Focus Area

By Marcus Ranum

SecurityFocus is very pleased to announce the roll-out of the new Firewalls focus area.

<http://www.securityfocus.com/columnists/165>

4. Welcome to the SecurityFocus Firewalls Focus Area

By Marcus Ranum

SecurityFocus is very pleased to announce the roll-out of the new Firewalls focus area.

<http://www.securityfocus.com/infocus/1700>

5. Welcome to the SecurityFocus Pen-Test Focus Area

By Ivan Arce

The new SecurityFocus Pen-Test focus area offers a unique forum for the exchange of pen-test information.

<http://www.securityfocus.com/infocus/1699>

II. BUGTRAQ SUMMARY

1. Cafelog b2 Remote File Include Vulnerability

BugTraq ID: 7738

Remote: Yes

Date Published: May 29 2003 12:00AM

Relevant URL:

<http://www.securityfocus.com/bid/7738>

Summary:

CafeLog b2 WebLog Tool allows users to generate news pages and weblogs dynamically. It is implemented in PHP and is available for a variety of platforms including Microsoft Windows.

A remote file include vulnerability has been reported for Cafelog. Due to insufficient sanitization of some user-supplied variables by the 'blogger-2-b2.php' and 'gm-2-b2.php' scripts, it is possible for a remote attacker to include a malicious PHP file in a URL.

An attacker may exploit this by supplying a path to a maliciously created file, located on an attacker-controlled host as a value for the '\$b2inc' parameter.

If the remote file is a malicious PHP script, this may allow for execution of attacker-supplied PHP code with the privileges of the web server.

Successful exploitation may provide local access to the attacker.

This vulnerability was reported for Cafelog 0.6.1.

2. Webfroot Shoutbox Remote Command Execution Vulnerability

BugTraq ID: 7746

Remote: Yes

Date Published: May 29 2003 12:00AM

Relevant URL:

<http://www.securityfocus.com/bid/7746>

Summary:

Webfroot Shoutbox is a web application designed to allow web site visitors a chance to leave messages. It is implemented in PHP and is available for a variety of platforms including Microsoft Windows.

Shoutbox is prone to an issue that may result in the execution of attacker-supplied code. The vulnerability exists due to insufficient sanitization of the 'conf' URI parameter.

An attacker can exploit this vulnerability to insert malicious PHP code into the web server logs which can then be executed by the PHP interpreter when the logs are requested. This will allow an attacker to execute arbitrary commands on a vulnerable system.

This vulnerability was reported to affect Webfroot Shoutbox 2.32 and earlier.

3. myServer HTTP GET Argument Buffer Overflow Vulnerability

BugTraq ID: 7770

Remote: Yes

Date Published: Jun 02 2003 12:00AM

Relevant URL:

<http://www.securityfocus.com/bid/7770>

Summary:

myServer is an application and web server for Microsoft Windows and Linux operating systems.

myServer has been reported prone to a remote buffer overflow vulnerability. The vulnerability exists when the web server attempts to process HTTP requests of excessive length. Specifically, when the web server processes an argument passed to a malicious HTTP GET request that consists of more than 4100+ bytes, the web server will crash. This will result in a denial of service condition.

It is possible that this vulnerability may also allow the execution of arbitrary instructions. Any instructions carried out through this vulnerability would be with the privileges of the web server process. However, the possibility of code execution has not been confirmed.

This vulnerability was reported for myServer version 0.4.1 It is likely that other versions are also affected.

4. Cafelog b2 B2MenuTop Script B2INC Variable Include Vulnerability BugTraq ID: 7786

Remote: Yes

Date Published: Jun 02 2003 12:00AM

Relevant URL:

<http://www.securityfocus.com/bid/7786>

Summary:

CafeLog b2 allows users to generate news pages and weblogs dynamically. It is implemented in PHP and is available for the Unix, Linux, and Microsoft Windows platforms.

A remote file include vulnerability has been reported in Cafelog b2. Due to insufficient sanitization of user-supplied values in the b2menutop.php script, it is possible for a remote attacker to influence the location of included files.

An attacker may exploit this by supplying a path to a maliciously created file, located on an attacker-controlled host as a value for the '\$b2inc' parameter.

If the remote file is a malicious PHP script, this may allow for execution of attacker-supplied PHP code with the privileges of the web server. Successful exploitation may provide local access to the attacker.

This vulnerability was reported for Cafelog 0.6.2.

5. Geeklog Image Upload Extension Validation Vulnerability

BugTraq ID: 7744

Remote: Yes

Date Published: May 29 2003 12:00AM

Relevant URL:

<http://www.securityfocus.com/bid/7744>

Summary:

Geeklog is open-source weblog software. It is written in PHP and will run on most Unix and Linux variants, as well as Microsoft Windows operating systems.

Geeklog allows weblog users to upload images. Uploaded images should have certain extensions (such as .jpg or .gif). However, Geeklog does not sufficiently validate image upload extensions. This issue exists in the users and stories modules. It may be possible for an attacker to upload a file with an arbitrary extension, such as a script, and then request the file.

Depending on web server configuration, this could result in execution of arbitrary commands or file corruption. More sophisticated attacks could

also occur, given that this vulnerability allows a remote attacker to place files with arbitrary extensions on the host.

6. Activity Monitor 2002 Remote Denial of Service Vulnerability

BugTraq ID: 7748

Remote: Yes

Date Published: May 29 2003 12:00AM

Relevant URL:

<http://www.securityfocus.com/bid/7748>

Summary:

Activity Monitor 2002 is an application designed to remotely monitor employee system usage. It is available for the Microsoft Windows operating system.

A vulnerability has been reported for Activity Monitor 2002 that may be exploited to remotely trigger a denial of service condition. The problem occurs while handling data received from hosts that are not registered in the Activity Monitor 'monitoring list'. Specifically if a host that is not being monitored by the Activity Monitor transmits an initial packet, with the SYN flag set, to the affected service via TCP port 15163 a packet with SYNACK flag set is sent back. This will cause an internal exception to occur in the Activity Monitor and the software will fail. Successive legitimate communications destined for this service will receive a RST as the port is now closed.

7. Pablo Software Solutions Baby POP3 Server Multiple Connection Denial Of Service Vulnerability

BugTraq ID: 7755

Remote: Yes

Date Published: May 29 2003 12:00AM

Relevant URL:

<http://www.securityfocus.com/bid/7755>

Summary:

Baby POP3 Server is a freely available, open source POP3 Server for the Microsoft Windows platform. It is maintained by Pablo Software Solutions.

A problem with the server may make it possible deny service to legitimate users of the host.

It has been reported that Baby POP3 Server does not properly handle large amounts of requests from one system. This may make it possible for a remote user cause a denial of service.

The problem is in the handling of a flood of connections from one system. When a single system attempts to open 100 or more connections to the POP3 Server, the server becomes unstable. It has been reported that this can reliably cause the server to throw an exception and crash.

8. Microsoft Internet Explorer False URL Information Vulnerability

BugTraq ID: 7763

Remote: Yes

Date Published: May 30 2003 12:00AM

Relevant URL:

<http://www.securityfocus.com/bid/7763>

Summary:

An issue has been reported for Microsoft Internet Explorer that may result in a false sense of security for a user.

Due to the way IE handles certain functions, the URL displayed on the 'location bar' will not correspond to the actual URL of the site displayed in the browser window. As a result, a malicious attacker can exploit this issue to entice a user to visit a web site and make them believe they are at known or trusted page.

9. WebCortex WebStores2000 SQL Injection Vulnerability

BugTraq ID: 7766

Remote: Yes

Date Published: May 31 2003 12:00AM

Relevant URL:

<http://www.securityfocus.com/bid/7766>

Summary:

WebCortex WebStores2000 is shopping cart software implemented in ASP. It is available for Microsoft Windows operating environments.

WebStores2000 has been reported to be prone to SQL injection attacks.

This vulnerability is reportedly caused by a lack of sufficient sanitization of user-supplied data contained in URI parameters supplied to WebStores2000. Specifically an attacker may inject SQL database commands by embedding malicious SQL commands within either the 'Item_ID' URI parameter, supplied to the browse_item_details.asp script.

Successful exploitation may allow for modification of the structure of SQL queries, resulting in information disclosure, or database corruption. The consequences depend on the nature of specific queries. This issue may allow the attacker to exploit latent vulnerabilities in the underlying database.

10. Gator EWallet Information Encoding Weakness

BugTraq ID: 7778

Remote: No

Date Published: Jun 02 2003 12:00AM

Relevant URL:

<http://www.securityfocus.com/bid/7778>

Summary:

Gator eWallet is software for managing personal data such as passwords and credit card information. It is available for Microsoft Windows operating systems.

Gator eWallet fails to adequately protect sensitive information stored by users.

Gator eWallet uses Base64 encoding to protect sensitive information. This information is stored in the following data files in the program folder:

mepgh.dat
mepcme.dat
meprca.dat
mepcmefc.dat
GMT.exe.manifest
meperr.dat
mepgus.dat
mepoem.dat
mepsnd-gs.dat
mepsnd-ksa.dat
mepcat.dat
sitehash4.dat

Local users with access to these files may gain access to a plethora of personal information. Base64 encoded data may be trivially reversed to obtain plaintext.

11. Microsoft Windows 2000/XP/2003 IPV6 ICMP Flood Denial Of Service Vulnerability

BugTraq ID: 7788

Remote: Yes

Date Published: Jun 02 2003 12:00AM

Relevant URL:

<http://www.securityfocus.com/bid/7788>

Summary:

Microsoft Windows 2000/XP/2003 has been reported prone to a remote denial of service vulnerability.

Reportedly, an attacker may trigger this vulnerability, under certain configurations. Specifically IPV6 must be enabled on the target server. Under these conditions an attacker may launch an ICMP flood attack, (An ICMP flood attack, by nature, is designed to send a greater number of ICMP echo request packets than the vulnerable protocol implementation can handle.), that could effectively deny network services to valid users.

Reportedly this issue is further exaggerated by bid 7666.

12. Microsoft Windows XP Nested Directory Denial of Service Vulnerability

BugTraq ID: 7789

Remote: No

Date Published: Jun 02 2003 12:00AM

Relevant URL:

<http://www.securityfocus.com/bid/7789>

Summary:

A vulnerability has been reported for all versions of Microsoft Windows XP. The problem occurs while handling the options menu of the last folder within 122 nested directories. The next directories must all use a naming scheme of strictly one character, such as 'a' or 'b'.

By moving the cursor over the menu for the 122nd folder it may be possible for an unprivileged local user to crash a target system.

13. IRCXpro Server Settings.INI Plaintext Password Storage Vulnerability

BugTraq ID: 7792

Remote: Yes

Date Published: Jun 03 2003 12:00AM

Relevant URL:

<http://www.securityfocus.com/bid/7792>

Summary:

IRCXpro Server is a IRC server that is designed for use with Microsoft Windows operating systems.

A problem with the IRCXpro Server could make unauthorized access to credentials possible.

It has been reported that a problem exists in the method used for the storage of passwords by IRCXpro. This could lead to local users gaining unauthorized access to passwords, and potentially unauthorized access to the vulnerable IRC server.

Specifically, IRCXpro Server stores user credentials in the "settings.ini" configuration file, using plain text format by default. A local user with sufficient privileges to read this file may obtain the usernames and passwords contained within.

Information gathered in this way may be used to aid in further attacks launched against the vulnerable system.

This vulnerability was reported for IRCXpro Server 1.0.

14. Pablo Software Solutions FTP Server Anonymous Users Privileges Vulnerability

BugTraq ID: 7799

Remote: Yes

Date Published: Jun 03 2003 12:00AM

Relevant URL:

<http://www.securityfocus.com/bid/7799>

Summary:

Pablo Software Solutions FTP Server is freely available software for Microsoft Windows operating systems.

An issue in Pablo FTP Service may make it possible for remote users to perform unauthorized actions.

It has been reported that Pablo FTP Service does not sufficiently restrict the anonymous user account, which is active by default. Because of this, a default configuration may provide a conduit for the disclosure of potentially sensitive information.

The problem is in the permission scheme implemented with a default installation. Reports indicate that the default anonymous account does not restrict the user from downloading files from any FTP server readable location on the affected system. By default the drive on which the software is installed is mapped readable from the root directory eg 'C:\'.

An attacker may exploit this vulnerability to access arbitrary files on the underlying system and potentially disclose sensitive information. Information gathered in this way may be harness in further attacks launched against the affected system.

It should be noted that while this vulnerability has been reported to affect Pablo FTP service version 1.2, other versions might also be affected.

15. Pablo Software Solutions FTP Server Plaintext Password Weakness BugTraq ID: 7801

Remote: No

Date Published: Jun 03 2003 12:00AM

Relevant URL:

<http://www.securityfocus.com/bid/7801>

Summary:

Pablo Software Solutions FTP Server is freely available software for Microsoft Windows operating systems.

An issue in Pablo FTP Service may make it possible for a user to access FTP account credentials.

It has been reported that Pablo FTP Service stores FTP User account passwords in plaintext format. As a result, these credentials could be exposed to other users. Passwords are stored in the 'users.dat' file. Any user who has read access to this file may retrieve Pablo FTP Service user account credentials.

This issue may be further exaggerated by BID 7799.

It should be noted that while this weakness has been reported to affect Pablo FTP service version 1.2, other versions might also be affected.

16. Webfroot Shoutbox URI Parameter File Disclosure Vulnerability

BugTraq ID: 7737

Remote: Yes

Date Published: May 29 2003 12:00AM

Relevant URL:

<http://www.securityfocus.com/bid/7737>

Summary:

Webfroot Shoutbox is a web application designed to allow web site visitors a chance to leave messages. It is implemented in PHP and is available for a variety of platforms including Microsoft Windows.

Shoutbox is prone to directory traversal attacks. The vulnerability exists due to insufficient sanitization of user-supplied values to URI parameters. Specifically, the 'conf' URI parameter is not sufficiently sanitized of '../' directory traversal sequences.

An attacker can exploit this vulnerability by manipulating the value of the 'conf' URI parameter to obtain any files readable by the web server.

Information obtained in this manner may allow an attacker to launch further, potentially destructive, attacks against a vulnerable system.

This vulnerability was reported to affect Webfroot Shoutbox 2.32 and earlier.

17. FrontRange Solutions GoldMine HTML Mail Script Execution Vulnerability

BugTraq ID: 7741

Remote: Yes

Date Published: May 29 2003 12:00AM

Relevant URL:

<http://www.securityfocus.com/bid/7741>

Summary:

FrontRange Solutions' GoldMine Business Contact Manager is an application to enable businesses to manage contacts. It is available for the Microsoft Windows operating system.

A vulnerability has been discovered in GoldMine that may result in the execution of malicious HTML and attacker-supplied code. The vulnerability exists due to the way GoldMine handles HTML e-mail. Specifically, any e-mail that includes HTML code will be sent directly to the default web browser (typically Internet Explorer) to be executed.

An attacker can exploit this vulnerability by creating a specially crafted e-mail and sending it to a vulnerable system. When the victim user views the e-mail using GoldMine, the malicious HTML code will be executed in the security context of the affected user.

It should be noted that a victim user does not have to open a malicious e-mail; this vulnerability will be triggered by simply previewing the

e-mail.

18. Geeklog Authentication SQL Injection Vulnerability

BugTraq ID: 7742

Remote: Yes

Date Published: May 29 2003 12:00AM

Relevant URL:

<http://www.securityfocus.com/bid/7742>

Summary:

Geeklog is open-source weblog software. It is written in PHP and will run on most Unix and Linux variants, as well as Microsoft Windows operating systems.

Geeklog is reported to be prone to SQL injection attacks during authentication. This is due to insufficient sanitization of cookie values, which will be used in database queries. This could permit an attacker to inject SQL code.

It has been demonstrated that vulnerability may allow a remote attacker to modify query logic and gain access to arbitrary Geeklog accounts, allowing for compromise of the software. It may also be possible, depending on the database implementation and other factors, to launch attacks against the database. This could result in disclosure of sensitive information or other consequences.

19. Pablo Software Solutions Baby FTP Server Directory Traversal Vulnerability

BugTraq ID: 7749

Remote: Yes

Date Published: May 29 2003 12:00AM

Relevant URL:

<http://www.securityfocus.com/bid/7749>

Summary:

Baby FTP Server is a freely available, open source FTP Server for the Microsoft Windows platform. It is maintained by Pablo Software Solutions.

A problem with the server may make it possible to gain unauthorized access to system resources.

It has been reported that Baby FTP Server does not properly handle some types of requests. This may make it possible for a remote user to gain access to resources outside of the FTP root directory.

The problem is in the handling of directory traversal strings. By executing the Change Working Directory (CWD) command with one of several known directory traversal strings, it is possible to escape the confines of the FTP directories and gain access to system files. The following strings will aid an attacker in escaping from the FTP root directory:

CWD ...
CWD /...
CWD /.....
CWD \...
CWD ...CWD .../

The attacker would have the privileges of the FTP server when traversing the file system.

20. Pablo Software Solutions Baby FTP Server Multiple Connection Denial Of Service Vulnerability

BugTraq ID: 7750

Remote: Yes

Date Published: May 29 2003 12:00AM

Relevant URL:

<http://www.securityfocus.com/bid/7750>

Summary:

Baby FTP Server is a freely available, open source FTP Server for the Microsoft Windows platform. It is maintained by Pablo Software Solutions.

A problem with the server may make it possible deny service to legitimate users of the host.

It has been reported that Baby FTP Server does not properly handle large amounts of requests from one system. This may make it possible for a remote user cause a denial of service.

The problem is in the handling of a flood of connections from one system. When a single system attempts to open 100 or more connections to the FTP Server, the server becomes unstable. It has been reported that this can reliably cause the server to throw an exception and crash.

21. Pablo Software Solutions Baby Web Server Multiple Connection Denial Of Service Vulnerability

BugTraq ID: 7752

Remote: Yes

Date Published: May 29 2003 12:00AM

Relevant URL:

<http://www.securityfocus.com/bid/7752>

Summary:

Baby Web Server is a freely available, open source Web Server for the Microsoft Windows platform. It is maintained by Pablo Software Solutions.

A problem with the server may make it possible deny service to legitimate users of the host.

It has been reported that Baby Web Server does not properly handle large amounts of requests from one system. This may make it possible for a remote user cause a denial of service.

The problem is in the handling of a flood of connections from one system. When a single system attempts to open 100 or more connections to the Web Server, the server becomes unstable. It has been reported that this can reliably cause the server to throw an exception and crash.

22. Pablo Software Solutions Quick and Easy FTP Server Denial Of Service Vulnerability

BugTraq ID: 7753

Remote: Yes

Date Published: May 29 2003 12:00AM

Relevant URL:

<http://www.securityfocus.com/bid/7753>

Summary:

Quick and Easy FTP Server is a freely available, open source FTP Server for the Microsoft Windows platform. It is maintained by Pablo Software Solutions.

A problem with the server may make it possible deny service to legitimate users of the host.

It has been reported that Quick and Easy FTP Server does not properly handle large amounts of requests from one system. This may make it possible for a remote user cause a denial of service.

The problem is in the handling of a flood of connections from one system. When a single system attempts to open 100 or more connections to the FTP Server, the server becomes unstable. It has been reported that this can reliably cause the server to throw an exception and crash.

23. Pablo Software Solutions Baby Web Server Directory Traversal Vulnerability

BugTraq ID: 7754

Remote: Yes

Date Published: May 29 2003 12:00AM

Relevant URL:

<http://www.securityfocus.com/bid/7754>

Summary:

Baby ASP Web Server is a freely available, open source Web Server for the Microsoft Windows platform. It is maintained by Pablo Software Solutions.

A problem with the server may make it possible to gain unauthorized access to system resources.

It has been reported that Baby ASP Web Server does not properly handle some types of requests. This may make it possible for a remote user to gain access to resources outside of the web root directory.

The problem is in the handling of directory traversal strings. By sending a request to the server with one of several known directory traversal

strings, it is possible to escape the confines of the web directories and gain access to system files. The following strings will aid an attacker in escaping from the web root directory:

```
../  
\\.
```

The attacker would have the privileges of the web server when traversing the file system.

24. Desktop Orbiter Resource Exhaustion Denial Of Service Vulnerability

BugTraq ID: 7759

Remote: Yes

Date Published: May 30 2003 12:00AM

Relevant URL:

<http://www.securityfocus.com/bid/7759>

Summary:

Desktop Orbiter is designed to be a desktop security solution. It is maintained by Anfibia and is available for the Microsoft Windows operating system.

A denial of service vulnerability has been reported for Desktop Orbiter. The vulnerability exists due to the way the application handles connections. Specifically, for every open connection, a snapshot preview of the desktop is loaded into memory. Thus, numerous connections would result in a consumption of all available memory resources.

An attacker can exploit this vulnerability by making numerous connections to a Desktop Orbiter server on TCP port 51054. For every connection, the vulnerable service creates a snapshot of the desktop that is subsequently loaded into memory. This will eventually result in the service consuming all available memory and causing the system to behave unpredictably.

This vulnerability affects Desktop Orbiter 2.01. It is not known whether earlier versions are affected.

25. PHP Transparent Session ID Cross Site Scripting Vulnerability

BugTraq ID: 7761

Remote: Yes

Date Published: May 30 2003 12:00AM

Relevant URL:

<http://www.securityfocus.com/bid/7761>

Summary:

PHP is a freely available, open source web scripting language package. It is available for Microsoft Windows, Linux, and Unix operating systems.

PHP contains an option known as transparent session IDs. This feature allows session IDs to be embedded with a URL.

A cross-site scripting vulnerability has been discovered in PHP version 4.3.1 and earlier. The problem occurs when the 'session.use_trans_sid' global parameter has been enabled.

Due to insufficient sanitization of the PHPSESSID URI parameter, it is possible for an attacker to embed malicious script code within a link. By embedding malicious code in such a way that an HTML tag will be prematurely terminated, it may be possible to execute arbitrary script code.

Successful exploitation of this issue would allow an attacker to execute arbitrary script code in a victim's browser within the context of the visited website. This may allow for the theft of sensitive information, such as session ID's, or possibly other attacks.

It should be noted that PHP versions prior to release 4.2.0 do not support transparent session IDs by default. Support must be specified during initial compilation.

26. iisCart2000 Arbitrary File Upload Vulnerability

BugTraq ID: 7765

Remote: Yes

Date Published: May 31 2003 12:00AM

Relevant URL:

<http://www.securityfocus.com/bid/7765>

Summary:

iisCart2000 is web-based shopping cart software implemented in ASP. It is available for the Microsoft Windows operating system.

A vulnerability has been reported for iisCart2000 that may result in an attacker uploading arbitrary files to a vulnerable server. The vulnerability exists in the upload.asp script. Specifically, the script does not properly verify that a user is authorized to upload files.

An attacker can exploit this vulnerability by issuing a request for the vulnerable script (residing in 'admin/' or './'). This will allow an attacker to upload arbitrary files to the vulnerable server. If the uploaded file is a ASP script file, it may be possible for an attacker to execute the uploaded script.

Successful exploitation may result in the execution of attacker-supplied code.

27. Microsoft URLScan Information Disclosure Weakness

BugTraq ID: 7767

Remote: Yes

Date Published: May 31 2003 12:00AM

Relevant URL:

<http://www.securityfocus.com/bid/7767>

Summary:

Microsoft URLScan is a tool that prevents certain types of specific HTTP requests from reaching a IIS (Internet Information Services) server.

A weakness has been reported for URLScan that may result in the disclosure of sensitive information.

The weakness exists because of the way URLScan handles HEAD HTTP requests. Specifically, when URLScan receives a HEAD request that is subsequently rejected, it is automatically converted to a GET request and sent to the underlying IIS server. This is so that the appropriate reject page is delivered to a requesting client.

The information returned may allow an attacker to identify systems that incorporate the use of URLScan.

28. WinMX Plaintext Password Storage Weakness

BugTraq ID: 7771

Remote: No

Date Published: Jun 02 2003 12:00AM

Relevant URL:

<http://www.securityfocus.com/bid/7771>

Summary:

WinMX is a P2P file sharing application for Microsoft Windows operating systems. It supports the OpenNap protocol and is compatible with a number of P2P servers.

WinMX stores P2P passwords in plaintext. As a result, these credentials could be exposed to other local users. Passwords are stored in the 'nservers.dat' file and are also be accessible to users via the server editing feature of the WinMX interface.

This issue has been reported in WinMX 2.6. It is thought that the issue may have been addressed in later versions, though no vendor confirmation is available.

29. Webfroot Shoutbox Expanded.PHP Remote Command Execution Vulnerability

BugTraq ID: 7772

Remote: Yes

Date Published: Jun 02 2003 12:00AM

Relevant URL:

<http://www.securityfocus.com/bid/7772>

Summary:

Webfroot Shoutbox is a web application designed to allow web site visitors a chance to leave messages. It is implemented in PHP and is available for the Unix, Linux, and Microsoft Windows platforms.

Shoutbox is prone to an issue that may result in the execution of attacker-supplied code. The vulnerability exists due to insufficient sanitization of input into the expanded.php script.

An attacker can exploit this vulnerability to insert malicious PHP code into the web server logs which can then be executed by the PHP interpreter when the logs are requested. This will allow an attacker to execute arbitrary commands on a vulnerable system in the context of the web server.

This vulnerability was reported to affect Webfroot Shoutbox 2.32 and earlier.

30. Webfroot Shoutbox Expanded.PHP Remote Directory Traversal Vulnerability

BugTraq ID: 7775

Remote: Yes

Date Published: Jun 02 2003 12:00AM

Relevant URL:

<http://www.securityfocus.com/bid/7775>

Summary:

Webfroot Shoutbox is a web application designed to allow web site visitors a chance to leave messages. It is implemented in PHP and is available for the Unix, Linux, and Microsoft Windows platforms.

A problem in Shoutbox may result in traversal attacks. The vulnerability exists due to insufficient sanitization of user-supplied values to the expanded.php script, and could allow the viewing of potentially sensitive files by attackers.

An attacker can exploit this vulnerability by manipulating the value of the 'conf' URI parameter submitted to the expanded.php script to obtain any files readable by the web server.

Information obtained in this manner may allow an attacker to launch further, potentially destructive attacks against a vulnerable system.

This vulnerability was reported to affect Webfroot Shoutbox 2.32 and earlier.

31. Cafelog b2 B2Functions Script B2INC Variable Include Vulnerability

BugTraq ID: 7782

Remote: Yes

Date Published: Jun 02 2003 12:00AM

Relevant URL:

<http://www.securityfocus.com/bid/7782>

Summary:

CafeLog b2 WebLog Tool allows users to generate news pages and weblogs dynamically. It is implemented in PHP and is available for the Unix, Linux, and Microsoft Windows platforms.

A remote file include vulnerability has been reported in Cafelog b2. Due to insufficient sanitization of user-supplied values by the

b2functions.php script, it is possible for a remote attacker to influence the location of included files.

An attacker may exploit this by supplying a path to a maliciously created file, located on an attacker-controlled host as a value for the '\$b2inc' parameter.

If the remote file is a malicious PHP script, this may allow for execution of attacker-supplied PHP code with the privileges of the web server. Successful exploitation may provide local access to the attacker.

This vulnerability was reported for Cafelog 0.6.1.

32. CafeLog b2 Blog.Header Script SQL Injection Vulnerability

BugTraq ID: 7783

Remote: Yes

Date Published: Jun 02 2003 12:00AM

Relevant URL:

<http://www.securityfocus.com/bid/7783>

Summary:

Cafelog b2 WebLog Tool allows users to generate news pages and weblogs dynamically. It is implemented in PHP and is available for the Unix, Linux, and Microsoft Windows platforms.

The Cafelog b2 tool does not properly sanitize user input sent to the blog.header.php script. Because of this, it is possible for an attacker to pass malicious SQL code to the underlying database.

The problems is in the checking of the \$posts variable of the script. SQL code may be inserted into the variable, and will in turn be executed by the database server. Requests could include adding, deleting, and modifying data. Additionally, this may allow a remote attacker to exploit vulnerabilities that exist in the underlying database.

33. Pi3Web SortName Buffer Overflow Vulnerability

BugTraq ID: 7787

Remote: Yes

Date Published: Jun 02 2003 12:00AM

Relevant URL:

<http://www.securityfocus.com/bid/7787>

Summary:

Pi3Web is a free, multi platform, configurable HTTP server and development environment. It is available for Unix/Linux variants and Microsoft Windows operating systems.

Pi3Web is prone to a buffer overflow vulnerability. This is due to insufficient bounds checking of URI parameters. It is possible to trigger this condition by specifying a 'SortName' URI parameter of excessive length. Excess data will overrun adjacent regions of memory. This

condition could be exploited to cause a denial of service or possibly to execute malicious instructions in the context of the server.

This issue was reported for Pi3Web 2.0.2 Beta 1 on Windows platforms.

It was originally believed that this condition only existed with certain indexing configurations but additional reports indicate that this is not the case.

III. MICROSOFT FOCUS LIST SUMMARY

1. Announcement: SecurityFocus Pen-Test and Firewalls Focus Areas (Thread)

Relevant URL:

<http://www.securityfocus.com/archive/88/323676>

2. SecurityFocus Microsoft Newsletter #139 (Thread)

Relevant URL:

<http://www.securityfocus.com/archive/88/323622>

3. Internet Explorer URL Spoofing Threat (Thread)

Relevant URL:

<http://www.securityfocus.com/archive/88/323315>

IV. NEW PRODUCTS FOR MICROSOFT PLATFORMS

1. OrangeBox Mail

by Cobion

Platforms: Windows 2000, Windows XP

Relevant URL:

http://www.cobion.com/index.php?l_ort=2002-03-06-16-42-31

Summary:

OrangeBox Mail prevents intellectual property, confidential documents, or offensive language from leaving the corporate domain via outgoing e-mail, while keeping spam or inappropriate content from coming in. Text of the message and all its attachments, regardless of format or compression, are analyzed and passed or blocked according to user-defined policy.

2. Restorer2000 Data Recovery Software

by BitMart Inc.

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

Relevant URL:

<http://www.bitmart.net/>

Summary:

BitMart Data Recovery Software Restorer2000 is one of the most powerful and cost effective undelete and data recovery software available on the market. It allows to undelete files, unerase, unformat, restore and

recover data from NTFS and FAT partitions even if they are damaged or deleted. It's quick and easy file recovery solution. Recover files with foreign-language filenames, long filenames, NTFS-compressed filenames, and alternative data streams such as Windows 2000 file information. SmartScan technology combined with the flexibility of adjusting parameters gives you full control over fast recovery procedure. Drive Image creation is very important and useful feature to recover data from drives with bad sectors. As long as your system's hardware is a functional, award winning Restorer2000 product may be the only solution you need for all your data recovery and undelete needs. With Restorer2000 you can quickly and easily restore your data saving your time, money and resources.

3. CyProtect File Encryption

by CyProtect AG

Platforms: Windows 2000, Windows XP

Relevant URL:

<http://english.cyprotect.com/main0113.php>

Summary:

CyProtect File Encryption is using the 256 bit polymorphic encryption algorithm to en- and decrypt files on your local hardisk or your network. A free decryption-only tool is added, so you can send it with encrypted files to another user via email.

V. NEW TOOLS FOR MICROSOFT PLATFORMS

1. LibTomCrypt v0.76

by Tom St Denis tomstdenis@iahu.ca

Relevant URL:

<http://www.libtomcrypt.org>

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

Summary:

LibTomCrypt is a comprehensive, modular, and portable cryptographic toolkit that provides developers with a vast array of well known published block ciphers, one-way hash functions, chaining modes, pseudo-random number generators, public key cryptography, and a plethora of other routines. It has been designed from the ground up to be very simple to use. It has a modular and standard API that allows new ciphers, hashes, and PRNGs to be added or removed without change to the overall end application. It features easy to use functions and a complete user manual which has many source snippet examples.

2. A Joint Monitoring System (AJMS) v1.8

by Andrew Gray

Relevant URL:

<http://www.argray.org/ams/>

Platforms: Java, Perl (any system supporting perl)

Summary:

AJMS (AKA "AMS") displays syslog messages in realtime via a browser or standalone Java client. It also supports searches of any SQL database. It offers straightforward configuration and integrates easily into any existing syslog environment.

3. Gherkin v0.2.2

by mschmuhl

Relevant URL:

<http://www.altmode.com/gherkin>

Platforms: Os Independent, POSIX

Summary:

Gherkin is a Web-enabled multi-threaded, centralized security scan manager that incorporates Nessus vulnerability scanning, DNS and nmblookup name resolution, nmap fingerprinting and scanning, and customized traceroute-based network node detection.

VI. SPONSOR INFORMATION

This issue brought to you by: SPI Dynamics

FREE White Paper: "How A Hacker Launches A Web Application Attack!"

Learn why 70% of today's successful hacks involve Web Application attacks such as: SQL Injection, XSS, Cookie Manipulation, and Parameter Manipulation. All undetectable by Firewalls and IDS! Download *FREE* white paper from SPI Dynamics for a complete guide to protection!

<http://www.securityfocus.com/SPIDynamics-ms-secnews2>

