

SecurityFocus Microsoft Newsletter #139

Source: <http://www.derkeiler.com/Mailing-Lists/securityfocus/focus-ms/2003-06/0001.html>

From: Marc Fossi (mfossi_at_securityfocus.com)

Date: 06/03/03

Date: Mon, 2 Jun 2003 18:31:03 -0600 (MDT)

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

SecurityFocus Microsoft Newsletter #139

This Issue is Sponsored by: Interland

"For a limited time get 15% OFF Netscreen Firewalls and an additional 15% OFF any Windows 2000 Managed Dedicated Hosting Solution from Interland. Knowledgeable 24/7/365 Technical Support. Call 1-877-504-0091 for more details on how to protect your dedicated server."

Visit us at: <http://www.securityfocus.com/Interland-ms-secnews>

I. FRONT AND CENTER

1. ****Announcing the new SecurityFocus Pen-Test and Firewalls Focus Areas****
2. Malware Myths and Misinformation Part 2
3. A Special Needs Class
4. Untrustworthy Passport

II. MICROSOFT VULNERABILITY SUMMARY

1. Sun ONE Application Server Plaintext Password Vulnerability
2. Nessus LibNASL Arbitrary Code Execution Vulnerability
3. EServ Directory Indexing Vulnerability
4. EServ Unauthorized Proxy Access Vulnerability
5. TextPortal Undocumented Username / Password Weakness
6. IISProtect Web Administration Interface SQL Injection...
7. AnalogX Proxy URI Buffer Overflow Vulnerability
8. PostNuke Phoenix Main Modules Multiple Path Disclosure...
9. Platform Load Sharing Facility LSF_ENVDIR Local Command...
10. IISProtect Authentication Bypass Vulnerability
11. Batalla Naval Remote Buffer Overflow Vulnerability
12. Privatefirewall FIN/XMas Scan Traffic Handling Vulnerability
13. P-News Administrative Account Creation Vulnerability
14. Sun ONE Application Server Error Message Cross-Site Scripting...
15. ShareMailPro Username Identification Weakness
16. Apple QuickTime/Darwin Streaming Server QTSSReflector Module...
17. Apple QuickTime/Darwin Streaming MP3Broadcaster ID3 Tag...
18. Microsoft Internet Connection Firewall IPv6 Traffic Blocking...

19. PostNuke Phoenix Rating System Denial Of Service Vulnerability
20. Newsscript Administrative Privilege Elevation Vulnerability
21. Softrex Tornado WWW–Server File Disclosure Vulnerability
22. Softrex Tornado WWW–Server Buffer Overflow Vulnerability
23. Microsoft Internet Explorer Malformed JavaScript Denial of...
24. Magic Winmail Server USER POP3 Command Format String...
25. Sun ONE Application Server Source Disclosure Vulnerability
26. Multiple Vendor FTP Server File Disclosure Vulnerability
27. FastTrack P2P Supernode Packet Handler Buffer Overflow...
28. Remote PC Access Denial Of Service Vulnerability
29. Meteor FTP Server Username Information Disclosure Vulnerability
30. Sun One Application Server Request Logging Circumvention Weakness
31. Super–M Son hServer File Disclosure Vulnerability

III. MICROSOFT FOCUS LIST SUMMARY

1. Article Announcement: Malware Myths and Misinformation Part 2...
2. Article Announcement: Conducting a Security Audit: An...
3. SecurityFocus Microsoft Newsletter #138 (Thread)
4. Re[2]: Windows 2003 Server – MS Rulez? (Thread)
5. Windows 2003 Server – MS Rulez? (Thread)

IV. NEW PRODUCTS FOR MICROSOFT PLATFORMS

1. NetScreen–Remote
2. SecurPass Suite
3. CyberFusion

V. NEW TOOLS FOR MICROSOFT PLATFORMS

1. BCWipe v1.2–3
2. SSHTerm v0.1.4 beta
3. CryptoHeaven v2.2.5

VI. SPONSOR INFORMATION

I. FRONT AND CENTER

1. ** Announcing the new SecurityFocus Pen–Test and Firewalls Focus Areas **

In response to the ever evolving needs of the security community, SecurityFocus is very pleased to announce the release of two new focus areas effective June 2, 2003:

Pen–Test at <<http://www.securityfocus.com/pen-test>> and

Firewalls at <<http://www.securityfocus.com/firewalls>>

2. Malware Myths and Misinformation Part 2
By David Harley May 28, 2003

This article is the second of a three–part series looking at some of the myths and misconceptions that undermine anti–virus protection.

<http://www.securityfocus.com/infocus/1698>

3. A Special Needs Class
By George Smith

The University of Calgary's new course in virus-writing begs the question: is it a cheap publicity stunt or just boneheaded educating?

<http://www.securityfocus.com/columnists/164>

4. Untrustworthy Passport
by Yen-Ming Chen (yenming.chen@foundstone.com)

On May 7, 2003, yet another vulnerability[1,2,3] was found on Microsoft's Passport service, a single sign-on service for multiple Web sites including Microsoft's own Hotmail and Expedia.com. The vulnerability allows an attacker to gain control of any passport user's account by resetting her password simply by accessing a server response file (SRF) interface. Microsoft disabled the vulnerable feature in a few hours after the information went public. Some sources [4] claim federal regulators can fine Microsoft up to 22 trillion dollars, although that will be unlikely. Either way, the damage to Passport and Microsoft's perception of trustworthy computing has been done. In this article, we take a deeper look at the vulnerability from the perspective of a software development life cycle, its impact and how to monitor and fix such problem. We will also examine how the bug could have slipped through the cracks standard penetration testing methodologies and provide recommendations to harden the methodology.

<http://www.securityfocus.com/guest/20225>

II. BUGTRAQ SUMMARY

1. Sun ONE Application Server Plaintext Password Vulnerability

BugTraq ID: 7712

Remote: No

Date Published: May 27 2003 12:00AM

Relevant URL:

<http://www.securityfocus.com/bid/7712>

Summary:

Sun ONE Application Server is the application server solution distributed and maintained by Sun Microsystems. It is available for the Unix, Linux, and Microsoft platforms.

A problem with the Sun ONE Application 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 Sun ONE Application Server. This could lead to local users gaining unauthorized access to passwords, and potentially unauthorized access to the Sun ONE administrative server.

Specifically, Sun ONE Application Server stores administrative server credentials in the "statefile" file, using plaintext format by default. To further exaggerate this problem, the Sun ONE application is installed by

default into a folder that is world readable. A local user with access sufficient to read this file may disclose the usernames and passwords contained within.

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

It should be noted that although this vulnerability has been reported to affect Sun ONE Application Server version 7.0 on Windows platforms, previous versions might also be affected.

2. Nessus LibNASL Arbitrary Code Execution Vulnerability

BugTraq ID: 7664

Remote: Yes

Date Published: May 22 2003 12:00AM

Relevant URL:

<http://www.securityfocus.com/bid/7664>

Summary:

Nessus is a vulnerability scanning utility available for the Unix and Microsoft Windows operating systems. libnasl is a library used by Nessus to process NASL scripts.

Nessus has reported that various flaws have been discovered in the libnasl library. Amongst other functions, scanner_add_port(), insstr() and ftp_log_in() fail to sufficiently handle malformed parameters and may allow a script to break out of the established sandbox environment. As a result, it may be possible for a malicious Nessus plugin to execute arbitrary system commands with the privileges of Nessus the application, possibly root.

It should be noted that this malicious script must be a legitimate plugin which has been uploaded to the Nessus server. Furthermore, the affected Nessus application must have enabled the 'plugins_upload' option which is disabled by default.

The precise details regarding this vulnerability are currently unknown. This BID will be updated as further information becomes available.

Although unconfirmed, these vulnerabilities may be exploited to execute arbitrary attacker-supplied code.

This issue affects Nessus version 2.05 and earlier.

3. EServ Directory Indexing Vulnerability

BugTraq ID: 7669

Remote: Yes

Date Published: May 23 2003 12:00AM

Relevant URL:

<http://www.securityfocus.com/bid/7669>

Summary:

EServ is a combination Mail, News, Web, FTP and Proxy Server for Microsoft Windows systems.

EServ does not sufficiently prevent web users from being able to view directory indexes. This is reported to be an issue even when a directory has an index file. This may result in disclosure of sensitive information which may be useful in further attacks against the system.

4. EServ Unauthorized Proxy Access Vulnerability

BugTraq ID: 7670

Remote: Yes

Date Published: May 23 2003 12:00AM

Relevant URL:

<http://www.securityfocus.com/bid/7670>

Summary:

EServ is a combination Mail, News, Web, FTP and Proxy Server for Microsoft Windows systems.

EServ is prone to a vulnerability that may allow it to be used as a proxy by unauthorized remote users. This can occur even if a proxy authentication is required or the proxy service is disabled. Users can proxy request through port 80 if the proxy service is disabled. It has also been reported that the FTP proxy may also be abused in a similar manner.

5. TextPortal Undocumented Username / Password Weakness

BugTraq ID: 7673

Remote: Yes

Date Published: May 23 2003 12:00AM

Relevant URL:

<http://www.securityfocus.com/bid/7673>

Summary:

TextPortal is a web-based content management system implemented in PHP. It is available for a variety of platforms including Microsoft Windows and Linux and Unix variant operating environments.

A weakness has been reported for TextPortal that may allow an attacker to obtain unauthorized access. The issue exists due to a weak, undocumented password used for the default administrative user 'god2'.

TextPortal encrypts passwords using crypt and stores them in the 'db_ures\admin_pass.php' file. Specifically, the user 'god2' has a default undocumented password of '12345'.

Access to the 'god2' account could grant unauthorized administrative access to remote attackers.

Administrative privileges gained on target systems may allow attackers to corrupt configuration settings. Other attacks are also possible.

6. IISProtect Web Administration Interface SQL Injection Vulnerability

BugTraq ID: 7675

Remote: Yes

Date Published: May 23 2003 12:00AM

Relevant URL:

<http://www.securityfocus.com/bid/7675>

Summary:

iisProtect is a security product for Microsoft Windows that provides authentication based access control to protect web resources.

The IISProtect web administration interface is prone to an SQL injection vulnerability.

The interface fails to properly sanitize user-supplied input before including it in SQL queries. This could allow remote users to pass malicious SQL input to database queries, resulting in modification of query logic and other attacks.

Successful exploitation could result in a compromise of site integrity, disclosure or modification of data, or potential exploitation of vulnerabilities in the underlying database implementation. This could also be exploited to call stored procedures such as 'xp_cmdshell', to execute operating system commands.

It is not clear if the IISProtect web administration interface is enabled by default.

7. AnalogX Proxy URI Buffer Overflow Vulnerability

BugTraq ID: 7681

Remote: Yes

Date Published: May 26 2003 12:00AM

Relevant URL:

<http://www.securityfocus.com/bid/7681>

Summary:

AnalogX Proxy is proxy server software for Microsoft Windows operating systems.

AnalogX Proxy is prone to a buffer overflow due to insufficient bounds checking of client-supplied URIs. It is possible to trigger this condition by submitting a URI that is greater than 340 characters. Exploitation could allow an attacker to corrupt sensitive regions of memory with attacker-supplied values, which could result in execution of arbitrary code in the context of the AnalogX server.

This is similar to this issue described in BID 5139.

8. PostNuke Phoenix Main Modules Multiple Path Disclosure Vulnerabilities

BugTraq ID: 7693

Remote: Yes

Date Published: May 26 2003 12:00AM

Relevant URL:

<http://www.securityfocus.com/bid/7693>

Summary:

PostNuke is a web-based content management system. It is implemented in PHP and available for Unix/Linux variants and Microsoft Windows platforms.

Path disclosure vulnerabilities have been reported in modules which are included with PostNuke Phoenix. Affected modules include Downloads, Web_Links, Sections, FAQ, Search, Reviews and Glossary. The nature of these issues is poor handling of data supplied via URI parameters, causing error pages to be generated that contain the path to the installation root directory and other resources.

Exploitation of these issues may allow an attacker to gather sensitive information.

Some of these issues may be previously reported or exist in other content management systems such as PHP-Nuke or PHPBB, due to shared code.

9. Platform Load Sharing Facility LSF_ENVDIR Local Command Execution Vulnerability BugTraq ID: 7655

Remote: No

Date Published: May 22 2003 12:00AM

Relevant URL:

<http://www.securityfocus.com/bid/7655>

Summary:

Load Sharing Facility is a high availability and load balancing software package distributed and maintained by Platform. It is available for Unix, Linux, and Microsoft Windows.

A problem in the software for the Unix and Linux platform may make it possible for a local user to gain unauthorized privileges.

It has been reported that Load Sharing Facility (LSF) does not properly handle input in environment variables. Because of this, an attacker may be able to gain escalated privileges on a vulnerable system.

The problem is in the handling of environment variables. When the lsadmin program is executed, shortly after starting execution it calls the lim program. The path to this program is specified in the configuration file. However, it is possible to change the location that will be checked for this program by altering the LSF_ENVDIR environment variable to force lsadmin to look for the lim program in a different location. By doing so, it is possible to create a malicious copy of the lim program which would be executed with the privileges of the lsadmin program. The lsadmin program is typically installed with elevated privileges.

10. IISProtect Authentication Bypass Vulnerability

BugTraq ID: 7661

Remote: Yes

Date Published: May 22 2003 12:00AM

Relevant URL:

<http://www.securityfocus.com/bid/7661>

Summary:

iisProtect is a security product for Microsoft Windows that provides authentication based access control to protect web resources.

A vulnerability has been reported that may allow for iisProtect authentication to be circumvented by web users. It is possible to bypass authentication to gain access to web resources by submitting a request which URL encoded character representations. iisProtect fails to recognize these character representations, but the underlying IIS server will interpret them and serve the resource that is requested.

Remote attackers may exploit this issue to gain access to sensitive web resources, which could allow for other attacks which compromise web resources.

11. Batalla Naval Remote Buffer Overflow Vulnerability

BugTraq ID: 7699

Remote: Yes

Date Published: May 26 2003 12:00AM

Relevant URL:

<http://www.securityfocus.com/bid/7699>

Summary:

Batalla Naval is graphical naval battle game that can be played over a network. It is available for Unix/Linux variants and Microsoft Windows operating systems.

Batalla Naval is prone to a remotely exploitable buffer overflow when handling requests of excessive length. In particular, sending a string to the game server (gbnserv) that is 500 or more bytes in length may cause stack memory to be corrupted. This could allow for execution of malicious instructions in the context of the game server.

The game server listens on port 1995 by default.

12. Privatefirewall FIN/XMas Scan Traffic Handling Vulnerability

BugTraq ID: 7700

Remote: Yes

Date Published: May 24 2003 12:00AM

Relevant URL:

<http://www.securityfocus.com/bid/7700>

Summary:

Privatefirewall is a security software package distributed and maintained by Privacyware. It is available for the Microsoft Windows platform.

A problem with Privatefirewall may make it possible to bypass firewall policies.

It has been reported that Privatefirewall does not properly handle TCP traffic with certain flag settings. This may allow an attacker to circumvent firewall filtering.

The problem is in the parsing of traffic with FIN and Xmas tree flag settings. Privatefirewall does not correctly handle traffic with these specific flags set. These types of flags may be set during either port scanning, or other potentially malicious network activity such as back door communication.

It has been reported that Privatefirewall does not properly filter these types of traffic when the "Filter Internet Traffic" and "Deny Internet Traffic" configuration variables in Privatefirewall are selected. An attacker could circumvent both traffic policies.

13. P-News Administrative Account Creation Vulnerability

BugTraq ID: 7689

Remote: Yes

Date Published: May 24 2003 12:00AM

Relevant URL:

<http://www.securityfocus.com/bid/7689>

Summary:

P-News is a web-based news management system. It is implemented in PHP and available for Unix/Linux variants and Microsoft Windows operating systems.

A vulnerability has been reported that could enable a P-News member to create and access an administrative account. The flaw exists in the 'p-news.php' script. It is possible to inject malicious data into the 'Name' account editing input field. Exploitation could allow a member to compromise P-News.

This issue was reported in P-News 1.16. Other versions may also be affected.

14. Sun ONE Application Server Error Message Cross-Site Scripting Vulnerability

BugTraq ID: 7710

Remote: Yes

Date Published: May 27 2003 12:00AM

Relevant URL:

<http://www.securityfocus.com/bid/7710>

Summary:

Sun ONE Application Server is the application server solution distributed and maintained by Sun Microsystems. It is available for the Unix, Linux, and Microsoft platforms.

Sun ONE Application Server has been reported prone to a cross-site scripting vulnerability.

Sun ONE Application Server does not adequately filter script code from URL parameters, making it prone to cross-site scripting attacks.

Attacker-supplied script code may be included in a malicious link to a JSP application hosted on the vulnerable server. If the request triggers an error, the error message may contain the attacker-supplied script code, which in turn may be executed in the browser of the web user who visits the link. The code will be executed in the security context of the system running Sun ONE Application Server. Such a link might be included in a HTML e-mail or on a malicious web page.

This may enable a remote attacker to steal cookie-based authentication credentials from legitimate users.

It should be noted that although this vulnerability has been reported to affect Sun ONE Application Server 7.0 on Windows platforms, previous versions might also be affected.

15. ShareMailPro Username Identification Weakness

BugTraq ID: 7658

Remote: Yes

Date Published: May 22 2003 12:00AM

Relevant URL:

<http://www.securityfocus.com/bid/7658>

Summary:

ShareMailPro is an e-mail server solution designed for use with Microsoft Windows systems.

A weakness has been reported in ShareMailPro that may reveal the existence of usernames to remote attackers.

This weakness is due to the fact that ShareMailPro responds with different messages depending on whether a given username exists or not.

If an attacker connects with a non-existent username, the following message is displayed:

-ERR sorry , no such mailbox

An attacker may be able to use this information to launch further intelligent attacks against the server or to launch a brute force password attack against a known user name.

This vulnerability was reported for ShareMailPro 3.6.1.

16. Apple QuickTime/Darwin Streaming Server QTSSReflector Module Integer Overflow Vulnerability
BugTraq ID: 7659

Remote: Yes

Date Published: May 22 2003 12:00AM

Relevant URL:

<http://www.securityfocus.com/bid/7659>

Summary:

The Darwin/QuickTime Streaming Servers are used as a web interface for Streaming Server configuration. They are available for the Linux, Solaris, Microsoft Windows and MacOS X operating systems.

A vulnerability has been reported for Apple Quicktime/Darwin Streaming Server. The problem is said to occur within the QTSSReflector module while processing the ANNOUNCE command. Specifically, by specifying the Content-Length of an ANNOUNCE request to 0xffffffff (4294967295) it may be possible to overflow an unsigned integer. As a result, an unexpected calculation may occur within the affected module, causing the server to crash. Due to the nature of the value that is supplied to Content-Length, this issue may actually be a result of signed/unsigned variable mismatching. This behavior however has not been confirmed.

It should be noted that it has been speculated that this issue may be exploitable to corrupt process memory. If so, it may be possible for an attacker to overwrite sensitive values in an attempt to execute arbitrary instructions with the privileges of the server.

Apple has confirmed that this issue may be exploitable to trigger a denial of service. However, it is believed that remote exploitability is unlikely as it would require an administrator to manually configure the service to permit unauthenticated broadcasts.

17. Apple QuickTime/Darwin Streaming MP3Broadcaster ID3 Tag Handling Vulnerability
BugTraq ID: 7660

Remote: Yes

Date Published: May 22 2003 12:00AM

Relevant URL:

<http://www.securityfocus.com/bid/7660>

Summary:

The Apple QuickTime/Darwin MP3 Broadcaster is encoding software used to stream online broadcasts. They are available for the Linux, Solaris, Microsoft Windows and MacOS X operating systems.

MP3Broadcaster has been reported prone to a vulnerability when processing malformed ID3 tag information. The issue presents itself, under specific conditions, when the user invokes the MP3Broadcaster utility using the '-X -l' command line options, to generate a list based off malicious MP3 files. When a malformed integer within the ID3 data of a malicious MP3 file is processed, a miscalculation may occur which could potentially result in the corruption of process memory. This is likely due to

insufficient sanity checks performed when handling signed integer values contained within MP3 file ID3 tags.

Apple has confirmed that this issue may be exploitable to trigger a denial of service. However, it is believed that remote exploitability is unlikely, as it would require an administrator to manually configure the service to permit unauthenticated broadcasts.

18. Microsoft Internet Connection Firewall IPv6 Traffic Blocking Vulnerability

BugTraq ID: 7666

Remote: Yes

Date Published: May 22 2003 12:00AM

Relevant URL:

<http://www.securityfocus.com/bid/7666>

Summary:

Microsoft provides firewall capabilities using its Internet Connection Firewall (ICF).

An issue has been reported for systems that have enabled ICF whereby certain traffic may bypass existing firewall filters. Specifically, it has been reported the ICF fails to block IPv6 traffic.

This may result in an administrator having a false sense of security.

19. PostNuke Phoenix Rating System Denial Of Service Vulnerability

BugTraq ID: 7702

Remote: Yes

Date Published: May 26 2003 12:00AM

Relevant URL:

<http://www.securityfocus.com/bid/7702>

Summary:

PostNuke is a web-based content management system. It is implemented in PHP and available for Unix/Linux variants and Microsoft Windows platforms.

A problem in the software may make it possible to prevent access to sites by legitimate users.

It has been reported that the PostNuke rating system does not properly handle some submissions to the rating system. Because of this, a remote attacker may be able to submit a string that causes a denial of service to legitimate users.

The problem is in the handling of rating strings of excessive length. By submitting a maliciously crafted string, it is possible to cause the software to become unstable and potentially crash. It has been reported this can affect both the web server and database server under the PostNuke installation, though it's not entirely clear how.

20. Newsscript Administrative Privilege Elevation Vulnerability

BugTraq ID: 7705

Remote: Yes

Date Published: May 27 2003 12:00AM

Relevant URL:

<http://www.securityfocus.com/bid/7705>

Summary:

Newsscript is a web-based news management system. It is written in PHP and available for Unix/Linux variants and Microsoft Windows operating systems.

A vulnerability was reported in Newsscript that may permit an unauthorized member to increase their privilege level. The issue exists in the profile editing function of the 'write.php' script. This is due to insufficient validation of data supplied to account editing input fields of Newsscript. In particular, it is possible to include user database delimiters (<~>) when editing user profile properties. This could be used to add arbitrary data to a user record, including modification of the user's privilege level.

21. Softrex Tornado WWW-Server File Disclosure Vulnerability

BugTraq ID: 7715

Remote: Yes

Date Published: May 28 2003 12:00AM

Relevant URL:

<http://www.securityfocus.com/bid/7715>

Summary:

Softrex Tornado www-Server is a freely available web server designed for use with the Microsoft Windows operating system.

It has been announced that Tornado www-Server is vulnerable to a condition that may result in the disclosure of potentially sensitive information.

According to the report, Tornado www-Server does not perform sufficient sanitization on client requested paths which include "../" character sequences. It is possible for attackers to obtain files and directories outside of the established web root folder by exploiting this vulnerability.

Files disclosed as a result of successful exploitation could potentially contain sensitive information that would be useful in mounting further attacks against the system hosting the web forum software.

22. Softrex Tornado WWW-Server Buffer Overflow Vulnerability

BugTraq ID: 7716

Remote: Yes

Date Published: May 28 2003 12:00AM

Relevant URL:

<http://www.securityfocus.com/bid/7716>

Summary:

Softrex Tornado www-Server is a freely available web server designed for use with the Microsoft Windows operating system.

A buffer overflow vulnerability has been reported for Tornado www-Server. The vulnerability exists when Tornado processes overly long HTTP GET requests.

An attacker can exploit this vulnerability by issuing a malicious GET request to the vulnerable server consisting of at least 471 characters. When this request is processed, the server will crash thereby resulting in a denial of service.

Although unconfirmed, it may be possible to exploit this vulnerability to execute malicious attacker-supplied code.

This vulnerability was reported for Tornado www-Server 1.2.

23. Microsoft Internet Explorer Malformed JavaScript Denial of Service Vulnerability

BugTraq ID: 7706

Remote: Yes

Date Published: May 27 2003 12:00AM

Relevant URL:

<http://www.securityfocus.com/bid/7706>

Summary:

An issue has been reported in Microsoft Internet Explorer. It is possible for a malicious web page using JavaScript to crash the browser process.

When certain malformed or incomplete JavaScript statements are handled by the JavaScript interpreter, Internet Explorer will fail. This may be due to use of irregular statements with the quoteText() function, though this is unconfirmed.

With Internet Explorer 6, this condition will result in only the browser used to parse the JavaScript failing.

Precise technical details of this vulnerability are not currently known. This record will be updated when new information becomes available.

24. Magic Winmail Server USER POP3 Command Format String Vulnerability

BugTraq ID: 7667

Remote: Yes

Date Published: May 23 2003 12:00AM

Relevant URL:

<http://www.securityfocus.com/bid/7667>

Summary:

Magic Winmail Server is a e-mail server designed for use on Microsoft Windows operating environments.

A format string vulnerability has been reported for Magic Winmail Server when processing the USER POP3 command.

An attacker may exploit this vulnerability by connecting to the vulnerable mail server and issuing the USER command with malicious format string specifiers. When the command is processed, the malicious format string specifiers may be interpreted. As a result, it may be possible for sensitive locations in memory to be corrupted. This may ultimately result in the execution of attacker-supplied code.

This vulnerability was reported for Magic Winmail Server 2.3.

25. Sun ONE Application Server Source Disclosure Vulnerability

BugTraq ID: 7709

Remote: Yes

Date Published: May 27 2003 12:00AM

Relevant URL:

<http://www.securityfocus.com/bid/7709>

Summary:

Sun ONE Application Server is the application server solution distributed and maintained by Sun Microsystems. It is available for the Unix, Linux, and Microsoft platforms.

Sun ONE Application Server is prone to a source code disclosure vulnerability. This issue is due to handling of case in requests for resources. By changing the case of a file extension, the server may fail to interpret the script and instead serve it as a normal web resource. For example, if a JSP page is requested with the '.jsp' extension, it will be interpreted. However, if the same resource is requested using with an extension of '.JSP', it will not be interpreted by the server.

Script source code may contain sensitive information, such as database authentication credentials, which will be disclosed to a remote attacker if this issue is exploited.

This issue exists for Sun ONE Application Server on Microsoft Windows platforms. Previous versions may also be affected.

26. Multiple Vendor FTP Server File Disclosure Vulnerability

BugTraq ID: 7718

Remote: Yes

Date Published: May 28 2003 12:00AM

Relevant URL:

<http://www.securityfocus.com/bid/7718>

Summary:

VisNetic FTPServer is a secure FTP server distributed by Deerfield. Titan FTP Server is a FTP server distributed by South River Technologies. Both servers are available for Microsoft Windows operating systems.

It has been announced that VisNetic FTPServer and Titan FTP Server are vulnerable to a condition that may result in the disclosure of potentially sensitive information.

According to the report, the affected servers do not perform sufficient sanitization on client requested paths, which include "../" character sequences passed to 'quote stat' commands. It is possible for attackers to obtain information relating to files and directories outside of the established FTP root folder by exploiting this vulnerability.

Attackers may disclose information about the structure and layout of the target filesystem. This could potentially lead to the disclosure of sensitive information that would be useful in mounting further attacks against the system running the vulnerable software.

27. FastTrack P2P Supernode Packet Handler Buffer Overflow Vulnerability

BugTraq ID: 7680

Remote: Yes

Date Published: May 26 2003 12:00AM

Relevant URL:

<http://www.securityfocus.com/bid/7680>

Summary:

KaZaA, Grokster and Morpheus are file-sharing clients based on FastTrack P2P technologies. They will run on Microsoft Windows 9x/ME/NT/2000/XP systems. Ports also exist for variants of the Linux operating system.

FastTrack P2P Supernode Packet Handler has been reported prone to a buffer overflow vulnerability. The issue presents itself in the FastTrack Supernode packet handler. The handler does not perform sufficient bounds checking on Supernode entries received before they are copied into a reserved buffer in internal memory.

Specifically, when Supernode data extracted from certain FastTrack P2P network packets is passed to the affected FastTrack class and later copied into internal memory, excessive Supernode data (>200 entries) may overrun the boundary of the assigned buffer and corrupt adjacent memory. Memory adjacent to this buffer has been reported to contain values that are crucial to controlling memory management or program execution flow. Therefore it may be possible for a remote attacker to trigger a denial of service condition or ultimately seize control of the vulnerable application and have arbitrary attacker supplied code executed. Code execution would occur in the context of the user running an application that incorporates the vulnerable FastTrack P2P Packet Handler.

It should be noted that this vulnerability has been tested on KaZaA version 2.0.2. Other versions of KaZaA and similar file-sharing clients based on FastTrack P2P technology may also be affected.

28. Remote PC Access Denial Of Service Vulnerability

BugTraq ID: 7698

Remote: Yes

Date Published: May 26 2003 12:00AM

Relevant URL:

<http://www.securityfocus.com/bid/7698>

Summary:

Remote PC Access is a remote administration tool designed for Microsoft Windows platforms.

Remote PC Access has been reported to be prone to a denial of service vulnerability.

The issue, although unconfirmed is likely due to a lack of bounds checking performed by the Remote PC Access server on network communications received from the client. Specifically an attacker may craft an authorization packet and transmit it to the vulnerable server, after the initial authorization process has been completed the server will send data to the client. The attacker may copy the information received and re-transmit it back to the server. This has the invariable effect of causing the vulnerable PC Access server to behave in an unstable manner eventually leading to a fatal exception.

Although unconfirmed, due to the nature of this vulnerability, it may be possible for a remote attacker to supply and execute arbitrary code.

It should be noted that although this vulnerability has been reported to affect Remote PC Access version 2.2, previous versions might also be affected.

29. Meteor FTP Server Username Information Disclosure Vulnerability

BugTraq ID: 7707

Remote: Yes

Date Published: May 27 2003 12:00AM

Relevant URL:

<http://www.securityfocus.com/bid/7707>

Summary:

Meteor FTP Server is an FTP Server for Microsoft Windows operating systems.

It has been reported that Meteor FTP Server is prone to an information disclosure weakness.

The problem exists in the way the FTP server handles the authentication procedure. Specifically the FTP server returns a '530 Not logged on' error message to the console, if the username supplied is invalid, before disconnecting the user. An attacker may exploit this weakness to enumerate valid usernames.

It should be noted that although this weakness was reported to affect Meteor FTP server version 1.5, previous versions might also be affected.

30. Sun One Application Server Request Logging Circumvention Weakness

BugTraq ID: 7711

Remote: Yes

Date Published: May 27 2003 12:00AM

Relevant URL:

<http://www.securityfocus.com/bid/7711>

Summary:

Sun ONE Application Server is the application server solution distributed and maintained by Sun Microsystems. It is available for the Unix, Linux, and Microsoft platforms.

A problem with the software may make it possible to circumvent logging.

It has been reported that Sun ONE Application Server may not properly log requests under some circumstances. Because of this, an attacker may be able to obscure attacks from the view of administrators.

The problem is in the handling of extremely long requests. Sun ONE Application Server is capable of serving requests with lengths of up to 4096 bytes. However, the logging facility truncates requests at the length of 4042 bytes. An attacker could potentially embed a malicious request in the 54 unlogged bytes, obscuring the specifics of the attack from administrator view.

It has been reported that this problem affects Sun ONE Application Server on Microsoft Windows platforms. Versions prior to 7.0 may also be affected, but this has not been confirmed.

31. Super-M Son hServer File Disclosure Vulnerability

BugTraq ID: 7717

Remote: Yes

Date Published: May 28 2003 12:00AM

Relevant URL:

<http://www.securityfocus.com/bid/7717>

Summary:

Super-M Son hServer is a freely available web server designed for use with the Microsoft Windows operating system.

It has been announced that Super-M Son hServer is vulnerable to a condition that may result in the disclosure of potentially sensitive information.

According to the report, hServer does not perform sufficient sanitization on client requested paths which include ".|/" character sequences. It is possible for attackers to obtain files and directories outside of the established web root folder by exploiting this vulnerability.

Files disclosed as a result of successful exploitation could potentially contain sensitive information that would be useful in mounting further

attacks against the system hosting the web forum software.

III. MICROSOFT FOCUS LIST SUMMARY

1. Article Announcement: Malware Myths and Misinformation Part 2 (Thread)

Relevant URL:

<http://www.securityfocus.com/archive/88/323119>

2. Article Announcement: Conducting a Security Audit: An Introductory Overview (Thread)

Relevant URL:

<http://www.securityfocus.com/archive/88/322796>

3. SecurityFocus Microsoft Newsletter #138 (Thread)

Relevant URL:

<http://www.securityfocus.com/archive/88/322798>

4. Re[2]: Windows 2003 Server – MS Rulez? (Thread)

Relevant URL:

<http://www.securityfocus.com/archive/88/322721>

5. Windows 2003 Server – MS Rulez? (Thread)

Relevant URL:

<http://www.securityfocus.com/archive/88/322720>

IV. NEW PRODUCTS FOR MICROSOFT PLATFORMS

1. NetScreen–Remote

by NetScreen Technologies

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

Relevant URL:

http://www.netscreen.com/products/at_a_glance/netscreen_remote.jsp

Summary:

The NetScreen–Remote VPN client provides the critical ability for client–initiated Virtual Private Network (VPN) communication. NetScreen–Remote is ideal for "road warriors" needing to access mission–critical networks across an untrusted or public network as well as end–users within an enterprise environment that require a secure end–user–to–host connection. NetScreen–Remote, based on SafeNet's industry–leading VPN client software, runs on an end–user's computer and facilitates secure remote access to networks, devices, or other hosts. Security is achieved by using the IPSec protocol and Layer 2 Tunneling Protocol (L2TP), with Certificates as an additional option. In order to form a secure communications channel, this software must be used in conjunction with an IPSec gateway, such as NetScreen's line of integrated security systems and appliances, or another host running IPSec compatible

software, including other computers running NetScreen-Remote. NetScreen-Remote encrypted communications can be initiated in any IP network environment, be it an Ethernet LAN or dial-up modem connection.

2. SecurPass Suite

by Proginet Corp

Platforms: AIX, AS/400, HP-UX, Linux, Netware, OS/2, OS/390, RACF, Solaris, True64 UNIX, Windows 2000, Windows 95/98, Windows NT, Windows XP

Relevant URL:

<http://www.proginetuk.co.uk/products/securpass-home.htm>

Summary:

SecurPass suite may be installed together or stand-alone. SecurPass-Sync Password Synchronisation in the enterprise across multiple platforms & applications to enhance security & save helpdesk costs. Users have the same password to all applications & on all platforms with any change in one always propagated to all. Security is enhanced by enforcing better policies, removes the likelihood of users writing down passwords, users may be revoked, resumed or deleted instantly from all points of entry. SecurPass-Sync offers the advantages of single sign-on without the costs & complexities in implementation and with benefits typically seen within a few weeks. SecurPass-Reset Password Reset – user self-reset of passwords without helpdesk intervention in the enterprise to enhance security & save help desk calls in multi or single-platform environments. Resets are enabled via a browser-based self-help utility in accordance with enterprise security standards that ensure type & numbers of questions fit the needs. Users re-enable their own accounts if they have forgotten their passwords & accidentally get locked out. Enterprise & user efficiency is increased & the significant reduction in helpdesk calls will ensure a rapid ROI.

3. CyberFusion

by Proginet Corp

Platforms: AIX, HP-UX, Linux, OS/390, Solaris, SunOS, Windows 2000, Windows 95/98, Windows NT, Windows XP

Relevant URL:

<http://www.proginetuk.co.uk/products/cyberfusion/cyberfusion.htm>

Summary:

CyberFusion enables secure, reliable, scalable, automated and comprehensive end-to-end management for secure file transfer across an extensive range of disparate computing platforms, including all mainframes and client/server environments. CyberFusion also provides extensive auditing, reporting and monitoring of activity. Secure file transfers for data backup, data recovery, disaster recovery, data archiving, data warehouse and other purposes are all easily enabled using the many features which offer much more than basic secure FTP (SFTP) or Secure Shell (SSH). Standard FTP software is not the cheap option it appears when total cost of ownership (TCO) is properly examined and the improved computer security is taken into account.

V. NEW TOOLS FOR MICROSOFT PLATFORMS

1. BCWipe v1.2-3

by Jetico, Inc. support@jetico.com

Relevant URL:

<http://www.jetico.com/>

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

Summary:

The BCWipe utility is designed to securely delete files from the disk. Standard file deletion leaves the contents of the "deleted" file on your disk. Unless it has been overwritten by files subsequently saved, it can be recovered using standard disk utilities. Working quickly and integrated with Windows Shell, BCWipe shreds data in files so that they can not be recovered by any means. BCWipe software is a freeware for non-commercial and non-governmental use. Please, refer to BCWipe End-User license agreement for more information on licensing terms.

2. SSHTerm v0.1.4 beta

by Richard Pernavas

Relevant URL:

<http://www.sshtools.com/>

Platforms: Os Independent

Summary:

SSHTerm is a Java SSH client that provides a whole range of features, including port forwarding, password authentication, public-key authentication, ANSI/VT100/VT220/VT320 terminal, full clipboard support, record and playback input/output, and the ability to load/save connection settings to a file.

3. CryptoHeaven v2.2.5

by Marcin Kurzawa marcin@cryptoheaven.com

Relevant URL:

<http://www.cryptoheaven.com/>

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

Summary:

CryptoHeaven offers secure email and online file sharing/storage. Its main features are secure and highly encrypted services such as group collaboration, file sharing, email, online storage, and instant messaging. It integrates multi-user based security into email, instant messaging, and file storage and sharing in one unique package. It provides real time communication for text and data transfers in a multi-user secure environment. The security and usability of CryptoHeaven is well-balanced; even the no-so-technically oriented computer users can enjoy this crypto product with very high level of encryption.

VI. SPONSOR INFORMATION

This Issue is Sponsored by: Interland

SecurityFocus Microsoft: SecurityFocus Microsoft Newsletter #139

"For a limited time get 15% OFF Netscreen Firewalls and an additional 15% OFF any Windows 2000 Managed Dedicated Hosting Solution from Interland. Knowledgeable 24/7/365 Technical Support. Call 1-877-504-0091 for more details on how to protect your dedicated server."

Visit us at: <http://www.securityfocus.com/Interland-ms-secnews>
