

SecurityFocus Microsoft Newsletter #163

Source: <http://www.derkeiler.com/Mailing-Lists/securityfocus/focus-ms/2003-11/0094.html>

From: Marc Fossi (mfossi_at_securityfocus.com)

Date: 11/18/03

Date: Tue, 18 Nov 2003 07:00:14 -0700 (MST)

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

SecurityFocus Microsoft Newsletter #163

This Issue Sponsored by: RSA Conference 2004

Network with over 10,000 of the brightest minds in information security at the largest, most highly-anticipated industry event of the year. Don't miss RSA Conference 2004! Choose from over 200 class sessions and see demos from more than 250 industry vendors. If your job touches security, you need to be here. Learn more or register at:

http://www.securityfocus.com/sponsor/RSA_ms-secnews_031117 and use priority code SF4.

I. FRONT AND CENTER

1. Banking Scam Revealed
2. Electronic Voting Debacle
3. Proposed: a Bounty for Bugs

II. MICROSOFT VULNERABILITY SUMMARY

1. IBM DB2 Multiple Command-Line Format String Vulnerabilities
2. IBM DB2 Multiple Command-Line Argument Buffer Overflow Vulne...
3. phpBB Profile.PHP SQL Injection Vulnerability
4. Qualcomm Eudora Reply-to-all Buffer Overrun Vulnerability
5. TelCondex SimpleWebserver Directory Traversal Vulnerability
6. Bugzilla Javascript Buglists Remote Information Disclosure V...
7. Winace UnAce Command Line Argument Buffer Overflow Vulnerabi...
8. Microsoft FrontPage Server Extensions Remote Debug Buffer Ov...
9. Microsoft FrontPage Server Extensions SmartHTML Interpreter ...
10. Microsoft Internet Explorer DHTML Drag and Drop Local File S...
11. Microsoft Excel XLM Macro Security Level Bypass Vulnerabilit...
12. Microsoft Windows Workstation Service Remote Buffer Overflow...
13. Microsoft Internet Explorer XML Object Zone Restriction Bypa...
14. Microsoft Internet Explorer Script URL Cross-Domain Access V...
15. Microsoft Internet Explorer Function Pointer Override Cross-...
16. Microsoft Internet Explorer ExecCommand Cross-Domain Access ...
17. Opera Web Browser Opera: URI Handler Directory Traversal Vul...
18. Microsoft Internet Explorer file.writeline Local File Writin...
19. Qualcomm Eudora Spoofed Attachment Line Denial Of Service Vu...

20. Qualcomm Eudora Encrypted EMail Attachment/Image Storage Vul...
21. OpenSSH PAM Conversation Memory Scrubbing Weakness

III. MICROSOFT FOCUS LIST SUMMARY

1. Exchange question (Thread)
2. New Microsoft Exchange Server Vulnerability (Thread)
3. Exchange question :VSMail mx4 (Thread)
4. Webcast: Microsoft Security VP talks about what Micr... (Thread)
5. AD structure for a school environment (Thread)
6. Exchange SMTP Hole? (Thread)
7. Article Announcement: Proposed: a Bounty for Bugs (Thread)
8. AW: EXCHANGE SMTP HOLE? (Thread)
9. Risks posed by a: drive with IE in kiosk mode (Thread)
10. FTP server security. (Thread)
11. Win2003 RPC failure after Hotfix (Thread)
12. Roll up of facts: FW: Exchange SMTP Hole? (Thread)
13. MS event logging (Thread)
14. SecurityFocus Microsoft Newsletter #162 (Thread)
15. Allowing site redirection with URLScan (Thread)
16. Article Announcement: Reeducation Campaign (Thread)

IV. NEW PRODUCTS FOR MICROSOFT PLATFORMS

1. EnCase Enterprise Edition
2. SafeGuard PDA
3. The CyberAngel Security Software
4. Cyber-Ark Inter-Business Vault
5. EnCase Forensic Edition
6. OverflowGuard

V. NEW TOOLS FOR MICROSOFT PLATFORMS

1. OSIRIS v2.1.0
2. Glub Tech Secure FTP v2.0.11
3. Enigmail v0.82.0
4. GPA (GNU Privacy Assistant) v0.7.0
5. Anti-Spam SMTP Proxy v1.0.6
6. PipeACL tools v1.0

VI. SPONSOR INFORMATION

I. FRONT AND CENTER

1. Banking Scam Revealed
By Secure Science Corporation

A detailed analysis of the recent "phishing" scam that targeted Citibank customers. This paper describes the use of compromised hosts, Website redirection and the specifics of a unique bulk-mailing tool that has been repeatedly used in the recent rash of financial email scams.

<http://www.securityfocus.com/infocus/1745>

2. Electronic Voting Debacle
By Scott Granneman

Grave concerns over the security of electronic voting machines in the United States means the heart of American democracy is at risk. ... >>

<http://www.securityfocus.com/columnists/198>

3. Proposed: a Bounty for Bugs
By Mark Rasch

Instead of paying hard cash to punish computer criminals, vendors should reward grey hat hackers for responsibly finding and reporting the security holes that make cyber attacks possible.

<http://www.securityfocus.com/columnists/197>

II. MICROSOFT VULNERABILITY SUMMARY

1. IBM DB2 Multiple Command-line Format String Vulnerabilities

BugTraq ID: 8989

Remote: No

Date Published: Nov 07 2003

Relevant URL: <http://www.securityfocus.com/bid/8989>

Summary:

DB2 is the database implementation maintained and distributed by IBM. It is available for the UNIX, Linux, and Microsoft Windows platforms. The db2govd, db2start, and db2stop database components are typically installed setuid.

Multiple format string vulnerabilities have been discovered within the IBM DB2 database specifically within the aforementioned components. The problems occur due to erroneous usage of format-based functions and could potentially allow an attacker to gain elevated privileges on a local system.

The db2start and db2stop binaries are both prone to a format string bug when handling a basic command-line argument, for example `./dbstart %x`. The db2govd binary is prone to the condition when handling parameters passed as part of the 'validate garbage' and 'stop' options.

An attacker could potentially exploit one of these conditions by passing specially calculated format string sequences to a target program. When handled, the program may be controlled in such a way that arbitrary code may be executed. All instructions executed would be run with the privileges of the owner of the specific binary.

2. IBM DB2 Multiple Command-Line Argument Buffer Overflow Vulne...

BugTraq ID: 8990

Remote: No

Date Published: Nov 07 2003

Relevant URL: <http://www.securityfocus.com/bid/8990>

Summary:

DB2 is the database implementation maintained and distributed by IBM. It

is available for the UNIX, Linux, and Microsoft Windows platforms. The db2govd, db2start, and db2stop database components are typically installed setuid/setgid.

IBM DB2 has been reported to be prone to multiple buffer overflow vulnerabilities that present themselves in binaries that are shipped with DB2. The vulnerabilities are likely caused due to a lack of sufficient boundary checks performed on user-supplied command-line arguments before they are copied into a reserved buffer in memory. By supplying data that exceeds the size of the reserved memory buffer used to store command line arguments, a local attacker may overflow the bounds of the affected buffer and corrupt adjacent memory. Because this memory contains values that are crucial to controlling program execution flow, the attacker may influence the execution flow of the vulnerable binary into attacker-controlled memory.

It has been reported that arguments between 65 and 9901 bytes in size may trigger this issue in the respective vulnerable executables. Ultimately this may lead to the execution of arbitrary attacker-supplied instructions with elevated privileges.

Although this issue has been reported to affect IBM DB2 versions v7 and v8 other versions may also be affected.

3. phpBB Profile.PHP SQL Injection Vulnerability

BugTraq ID: 8994

Remote: Yes

Date Published: Nov 08 2003

Relevant URL: <http://www.securityfocus.com/bid/8994>

Summary:

phpBB is an open-source web forum application that is written in PHP and supported by a number of database products. It will run on most Unix and Linux variants, as well as Microsoft Windows operating systems.

A SQL injection vulnerability has been reported for phpBB systems.

phpBB, in some cases, does not sufficiently sanitize user-supplied input, which is used when constructing SQL queries to execute on the underlying database. As a result, it is possible to manipulate SQL queries. This may allow a remote attacker to modify query logic or potentially corrupt the database.

This vulnerability was reported to exist in the profile.php script file. A remote attacker can exploit this vulnerability by manipulating the \$u URI parameter to modify SQL query logic.

SQL injection attacks may also potentially be used to exploit latent vulnerabilities in the underlying database implementation.

It should be noted that although this vulnerability has been reported to affect phpBB version 2.0.5 and prior, it may also affect version 2.0.6.

4. Qualcomm Eudora Reply-to-all Buffer Overrun Vulnerability

BugTraq ID: 8997

Remote: Yes

Date Published: Nov 10 2003

Relevant URL: <http://www.securityfocus.com/bid/8997>

Summary:

Eudora is an e-mail client for Microsoft Windows and other operating systems. It is maintained and distributed by Qualcomm.

Qualcomm Eudora is prone to a buffer overrun when performing reply-to-all operations with message header fields (such as "From" or "Reply-To") of excessive length. To exploit this issue, an attacker must send a malicious message to a user of the client, which the user must then respond to using the reply-to-all. When the malformed message header fields are processed, adjacent regions of memory will be corrupted with attacker-supplied values. In this manner it may be possible to control execution flow and execute arbitrary code in the context of the client user.

This issue was reported to affect Windows versions of the software. It is not known if other platforms are similarly affected.

5. TelCondex SimpleWebserver Directory Traversal Vulnerability

BugTraq ID: 8998

Remote: Yes

Date Published: Nov 10 2003

Relevant URL: <http://www.securityfocus.com/bid/8998>

Summary:

TelCondex SimpleWebServer is a Web server designed for use with the Microsoft Windows operating systems.

A vulnerability has been reported to exist in the software that may allow a remote attacker to access information outside the server root directory. The problem exists due to insufficient sanitization of user-supplied data. The issue may allow a remote attacker to traverse outside the server root directory by using '.../' character sequences.

Successful exploitation of this vulnerability may allow a remote attacker to gain access to sensitive information that may be used to launch further attacks against a vulnerable system.

TelCondex SimpleWebserver version 2.13.31027 build 3289 is reported to be prone to this issue, however other versions may be affected as well.

6. Bugzilla Javascript Buglists Remote Information Disclosure V...

BugTraq ID: 9001

Remote: Yes

Date Published: Nov 10 2003

Relevant URL: <http://www.securityfocus.com/bid/9001>

Summary:

Bugzilla is a freely available, open source bug tracking system. It is

available for the Unix, Linux, and Microsoft Windows platforms.

A problem exists in the handling of buglists by Bugzilla when the lists are implemented with Javascript. Because of this, a remote user may be able to gain unauthorized access to sensitive information.

The problem is in the storage of information when placed in Javascript arrays. It is possible for a remote user to create a buglink in their page that correctly reflects information about a bug, including details which may be restricted from the public due to sensitivity of information. This may result in unauthorized disclosure of information.

This problem has also been reported to affect bookmarklets. The issue is known to affect version 2.7.15 only.

7. Winace UnAce Command Line Argument Buffer Overflow Vulnerabi...

BugTraq ID: 9002

Remote: Yes

Date Published: Nov 10 2003

Relevant URL: <http://www.securityfocus.com/bid/9002>

Summary:

Winace is a file compression/decompression tool that was originally developed for Microsoft Windows platforms. Winace was ported to Linux platforms as UnAce.

UnAce has been reported to be prone to a buffer overflow vulnerability. The issue presents itself when UnAce handles ace filenames that are greater than 610 bytes in length including the ace file extension. When this filename is passed to the UnAce utility as an argument for the 'e' (extract command line switch), the string is copied into a reserved buffer in memory. Data that exceeds the size of the reserved buffer will overflow its bounds and will trample any saved data that is adjacent to the affected buffer. Because variables that are crucial to controlling program execution flow for UnAce are conjectured to be stored adjacent to the affected buffer, an attacker may corrupt these values and influence UnAce program execution flow into attacker controlled memory. Ultimately this may lead to the execution of arbitrary instructions in the context of the user who is running UnAce.

If UnAce is associated with a specific file type in for example an Internet browser, clicking on a malicious ace filename may be sufficient to result in the execution of arbitrary instructions on an affected host.

8. Microsoft FrontPage Server Extensions Remote Debug Buffer Ov...

BugTraq ID: 9007

Remote: Yes

Date Published: Nov 11 2003

Relevant URL: <http://www.securityfocus.com/bid/9007>

Summary:

FrontPage Server Extensions are a component for FrontPage that allows authorized users to edit and maintain content.

FrontPage Server Extensions includes remote debugging functionality, allowing users to connect to the server to debug content using software such as Visual Interdev. A remotely exploitable buffer overrun vulnerability has been reported in the remote debugging functionality provided by the software.

This issue is due to an unchecked buffer size in a .DLL (fp30reg.dll) included with the extensions. It is possible to trigger this issue by sending a malformed chunked-encoded HTTP POST request. This will allow the attacker to influence the values in the ECX and EDI registers, which may be leveraged to execute arbitrary code. Exploitation may allow a remote attacker to execute arbitrary code on a vulnerable system with Local System privileges.

9. Microsoft FrontPage Server Extensions SmartHTML Interpreter ...

BugTraq ID: 9008

Remote: Yes

Date Published: Nov 11 2003

Relevant URL: <http://www.securityfocus.com/bid/9008>

Summary:

FrontPage Server Extensions are a component for FrontPage that allows authorized users to edit and maintain content. FrontPage

FrontPage Server Extensions include the SmartHTML interpreter, which allows web pages to access various FrontPage features. A denial of service vulnerability has been reported in the SmartHTML interpreter that may be exploited by remote attackers. It is possible to send an invalid request that will cause the interpreter to cycle, denying availability of CPU resources. In this manner, it is possible to cause a denial of service by exhausting available resources on the system.

10. Microsoft Internet Explorer DHTML Drag and Drop Local File S...

BugTraq ID: 9009

Remote: Yes

Date Published: Nov 11 2003

Relevant URL: <http://www.securityfocus.com/bid/9009>

Summary:

Microsoft has announced a vulnerability in Internet Explorer when handling specific DHTML events. Specifically, the problem is said to occur due when Internet Explorer handles Drag and Drop event. Following such a link is said to allow an arbitrary file to be dropped (saved) to the users local filesystem. The user will not be prompted in any way when this occurs.

Successful exploitation of this condition could ultimately allow an attacker to trigger the execution of arbitrary code with the privileges of the user. This could be possibly accomplished by dropping the malicious executable into the systems startup directory, or other sensitive locations on the system.

Microsoft has stated that dropping the executable to specific locations on the system may trigger the immediate execution of the file.

This vulnerability can be exploited via a malicious web page or via malicious HTML e-mail. Other applications that use the Internet Explorer engine are affected as well (Outlook, MSN Messenger, etc.).

11. Microsoft Excel XLM Macro Security Level Bypass Vulnerabilit...

BugTraq ID: 9010

Remote: Yes

Date Published: Nov 11 2003

Relevant URL: <http://www.securityfocus.com/bid/9010>

Summary:

Microsoft Excel contains a macro security feature. This feature scans a document when a user opens it to determine if there are any embedded macros. Then, depending on the security setting, the user is prompted whether or not to allow the macro to run, or the macro is executed automatically depending on user settings.

A vulnerability has been reported to affect Microsoft Excel that could be exploited by an attacker to execute an XLM [Excel 4] macro regardless of the macro security level. The issue has been reported to present itself due to a failure by Excel to sufficiently scan a malicious spreadsheet file before opening it. As a result of this failure an XLM macro embedded in a malicious spreadsheet will be executed when the document is opened, without Excel presenting a macro security warning and regardless of Excel macro security settings. Macro code execution will occur in the context of the user who is running the vulnerable version of Excel and could ultimately allow an attacker to perform arbitrary scripted tasks with administrative privileges.

12. Microsoft Windows Workstation Service Remote Buffer Overflow...

BugTraq ID: 9011

Remote: Yes

Date Published: Nov 11 2003

Relevant URL: <http://www.securityfocus.com/bid/9011>

Summary:

A vulnerability in Microsoft Windows Workstation service has been reported. Because of this issue, it may be possible for a remote attacker to gain unauthorized access to a vulnerable host.

The problem is in the handling of requests by the Workstation Service (WKSSVC.DLL). The Workstation Service is accessed by a remote system through Remote Procedure Call (RPC). RPC is handled through services listening on TCP and UDP ports 138, 139, and 445.

The Workstation Service does not properly check bounds on remote data. Because of this, it is possible to overwrite sensitive regions of system memory. The problem exists due to insufficient bounds checking in the network management functions provided through the DCE/RPC service. Some of these management events generate a logfile in the 'Debug' subdirectory within the Windows installation folder. When log entries are created, the logging function in 'WKSSVC.DLL' calls the 'vsprintf' routine without performing bounds checking. Therefore, if an exceptionally long string is

provided as a parameter to an RPC function that writes it to the log file, a stack-based buffer overflow will occur.

This issue could be exploited by a remote user to execute code with the privileges of the Workstation Service, which is typically invoked with SYSTEM privileges.

13. Microsoft Internet Explorer XML Object Zone Restriction Bypa...

BugTraq ID: 9012

Remote: Yes

Date Published: Nov 11 2003

Relevant URL: <http://www.securityfocus.com/bid/9012>

Summary:

Microsoft has announced that a vulnerability exists in Internet Explorer when handling malicious XML objects. This issue affects Microsoft Internet Explorer 5.5 to 6.0.

The vulnerability is said to occur due to Internet Explorer failing to validate the path to which an XML object is bound, making it possible to access the contents of files outside of the current zone. As a result, it may be possible for an attacker to expose the contents of a victim's local file system, despite the object being within the Internet or Intranet zone.

Microsoft has stated that, when a victim user visits a website containing the malformed object, they will be prompted to download an HTML file. Only when this file is downloaded will exploitation occur.

Successful exploitation of this issue could result in an attacker disclosing sensitive information from a users system. This data could possibly aid in launching future attacks against the user or systems to which they have access.

This vulnerability can be exploited via a malicious web page or via malicious HTML e-mail. Other applications that use the Internet Explorer engine are affected as well (Outlook, MSN Messenger, etc.).

14. Microsoft Internet Explorer Script URL Cross-Domain Access V...

BugTraq ID: 9013

Remote: Yes

Date Published: Nov 11 2003

Relevant URL: <http://www.securityfocus.com/bid/9013>

Summary:

An issue has been reported in Microsoft Internet Explorer that could allow malicious script code from one domain to be executed in the context of another domain.

The issue exists because the Script URL method is able to bypass cross-domain security checks performed by Internet Explorer.

This vulnerability could allow a web page from one domain to access information from another domain, including the local system. Additionally, a remote attacker could run any executable file on the local system, though this would require exploitation of multiple vulnerabilities in tandem.

Further information has been made available stating that this issue was discovered by Liu Die Yu and publicly known prior to the release of MS03-048. This issue was originally described as one of the vulnerabilities in BID 8577 "Multiple Microsoft Internet Explorer Script Execution Vulnerabilities". This new information is currently under investigation, this BID will be updated with specific technical details when analysis is complete.

15. Microsoft Internet Explorer Function Pointer Override Cross-...

BugTraq ID: 9014

Remote: Yes

Date Published: Nov 11 2003

Relevant URL: <http://www.securityfocus.com/bid/9014>

Summary:

An issue has been reported in Microsoft Internet Explorer that could allow malicious script code from one domain to be executed in the context of another domain.

The issue exists because the Function Pointer Override method is able to bypass cross-domain security checks performed by Internet Explorer.

This vulnerability could allow a web page from one domain to access information from another domain, including the local system. Additionally, a remote attacker could run any executable file on the local system, though this would require exploitation of multiple vulnerabilities in tandem.

Further information has been made available stating that this issue was discovered by Liu Die Yu and publicly known prior to the release of MS03-048. This issue was originally described as one of the vulnerabilities in BID 8577 "Multiple Microsoft Internet Explorer Script Execution Vulnerabilities". This new information is currently under investigation, this BID will be updated with specific technical details when analysis is complete.

16. Microsoft Internet Explorer ExecCommand Cross-Domain Access ...

BugTraq ID: 9015

Remote: Yes

Date Published: Nov 11 2003

Relevant URL: <http://www.securityfocus.com/bid/9015>

Summary:

An issue has been reported in Microsoft Internet Explorer that could allow malicious script code from one domain to be executed in the context of another domain.

The issue exists because the ExecCommand method is able to bypass cross-domain security checks performed by Internet Explorer.

This vulnerability could allow a web page from one domain to access information from another domain, including the local system. Additionally, a remote attacker could run any executable file on the local system, though this would require exploitation of multiple vulnerabilities in tandem.

Further information has been made available stating that this issue was discovered by Liu Die Yu and publicly known prior to the release of MS03-048. This issue was originally described as one of the vulnerabilities in BID 8577 "Multiple Microsoft Internet Explorer Script Execution Vulnerabilities". This new information is currently under investigation, this BID will be updated with specific technical details when analysis is complete.

17. Opera Web Browser Opera: URI Handler Directory Traversal Vul...

BugTraq ID: 9021

Remote: Yes

Date Published: Nov 12 2003

Relevant URL: <http://www.securityfocus.com/bid/9021>

Summary:

Opera is a web browser available for a number of platforms, including Microsoft Windows, Linux and Unix variants and Apple MacOS.

Opera uses an internal URI handler called 'Opera:' or 'about:' to display help files and other documentation. Common uses for this command include "opera:history", "opera:plugins", "opera:cache", and "opera:drives". A vulnerability has been reported to exist in the software that may allow an attacker to access information outside the intended directories for help files and documentation. The problem exists due to insufficient sanitization of user-supplied data through the 'Opera:' URI handler. The issue may allow an attacker to traverse the client file system by using '..%5c' or '..%2f' character sequences.

Successful exploitation of this vulnerability may allow an attacker to gain access to sensitive information that may be used to launch further attacks against a vulnerable system.

It has been reported that this issue may be exploited with another issue described in BID 9019 to drop files onto a client system in a predictable location and cause these files to be executed.

Opera Web Browser versions 7.21 and prior are reported to be prone to this issue. This issue was reported to exist in Windows versions of the web browser. It is not known if versions for other platforms are similarly affected.

18. Microsoft Internet Explorer file.writeline Local File Writin...

BugTraq ID: 9022

Remote: Yes

Date Published: Nov 12 2003

Relevant URL: <http://www.securityfocus.com/bid/9022>

Summary:

A problem has been reported in the handling of the file.writeline function in Microsoft Internet Explorer. Because of this, it may be possible for an attacker to write a file to a known location.

Reports indicate that under some circumstances, the Javascript file.writeline method is not properly restricted by the browser. When the method is invoked by a remote site, it is possible to write potentially malicious HTML or script code into a file on the system. The file could be written in a location that is predictable or known.

The attacker could take advantage of this issue to execute the file containing attacker-supplied content through another bug that allows the execution of the file on the local host. By doing so, the attacker could potentially execute code on the local system with the privileges of the user of the web browser.

This problem is known to affect Internet Explorer versions 5.0. It is not currently known what other, if any, versions are also affected by this issue.

19. Qualcomm Eudora Spoofed Attachment Line Denial Of Service Vu...

BugTraq ID: 9026

Remote: Yes

Date Published: Nov 12 2003

Relevant URL: <http://www.securityfocus.com/bid/9026>

Summary:

Eudora is an e-mail client for Microsoft Windows and other operating systems. It is maintained and distributed by Qualcomm.

A vulnerability has been reported by Qualcomm that may be exploited by a remote attacker to cause the Eudora e-mail client to crash. The issue has been reported to present itself within procedures employed by Eudora to handle attachment converted lines. It has been reported that a malicious email that contains a spoofed attachment converted line will trigger this issue in a vulnerable release of Eudora when the malicious message is viewed.

A remote attacker may exploit this issue to crash a remote users Eudora client; this may result in a loss of data.

20. Qualcomm Eudora Encrypted EMail Attachment/Image Storage Vul...

BugTraq ID: 9028

Remote: No

Date Published: Nov 12 2003

Relevant URL: <http://www.securityfocus.com/bid/9028>

Summary:

Eudora is an e-mail client for Microsoft Windows and other operating

systems. It is maintained and distributed by Qualcomm.

Eudora has been reported to be prone to a vulnerability that presents itself during email decryption procedures. Qualcomm has reported that when an encrypted email is decrypted, images that are embedded in the body of the email and attachments of the email are stored in a decrypted format on the local hard drive. This vulnerability presents itself even if the user explicitly chooses not to save the decrypted message text.

A local attacker who has sufficient access to read the saved images and attachments may potentially reveal confidential data that was intended to be obfuscated from third parties.

Information harvested in this manner could potentially be used to mount further attacks against the victim.

21. OpenSSH PAM Conversation Memory Scrubbing Weakness

BugTraq ID: 9040

Remote: No

Date Published: Nov 13 2003

Relevant URL: <http://www.securityfocus.com/bid/9040>

Summary:

OpenSSH is a freely available, open source implementation of the Secure Shell protocol. It is available for the Unix, Linux, and Microsoft platforms.

An issue has been reported in the OpenSSH implementation of PAM conversation functions. Applications which use PAM modules for authentication are required to include conversation routines to manage communications between the application and the PAM module, providing a means to prompt users for passwords or provide other functionality which relies on PAM. When a remote user connects to an OpenSSH server and prematurely cancels the connection through a function such as Control-C, OpenSSH does not correctly respond. It has been reported that OpenSSH ends the session with the `pam_end()` function rather than returning `PAM_CONV_ERR`, which is the correct behavior according to the Linux-PAM developer documentation. As a result, PAM will not handle the aborted conversation correctly and subsequently fail to scrub memory. The direct consequence is that sensitive information in memory is more likely to end up in swap space or core dumps.

This problem may expose authentication credentials to recovery should an attacker have sufficient privileges on the system to view core dumps or system memory. This issue may also expose other vulnerabilities in PAM modules due to unpredictable behavior that could potentially lead to stability issues and the compromise of sensitive credentials, information, or privileges.

III. MICROSOFT FOCUS LIST SUMMARY

1. Exchange question (Thread)

Relevant URL:

<http://www.securityfocus.com/archive/88/344582>

2. New Microsoft Exchange Server Vulnerability (Thread)

Relevant URL:

<http://www.securityfocus.com/archive/88/344581>

3. Exchange question :VSMail mx4 (Thread)

Relevant URL:

<http://www.securityfocus.com/archive/88/344570>

4. Webcast: Microsoft Security VP talks about what Micr... (Thread)

Relevant URL:

<http://www.securityfocus.com/archive/88/344569>

5. AD structure for a school environment (Thread)

Relevant URL:

<http://www.securityfocus.com/archive/88/344472>

6. Exchange SMTP Hole? (Thread)

Relevant URL:

<http://www.securityfocus.com/archive/88/344469>

7. Article Announcement: Proposed: a Bounty for Bugs (Thread)

Relevant URL:

<http://www.securityfocus.com/archive/88/344424>

8. AW: EXCHANGE SMTP HOLE? (Thread)

Relevant URL:

<http://www.securityfocus.com/archive/88/344420>

9. Risks posed by a: drive with IE in kiosk mode (Thread)

Relevant URL:

<http://www.securityfocus.com/archive/88/344415>

10. FTP server security. (Thread)

Relevant URL:

<http://www.securityfocus.com/archive/88/344414>

11. Win2003 RPC failure after Hotfix (Thread)

Relevant URL:

<http://www.securityfocus.com/archive/88/344413>

12. Roll up of facts: FW: Exchange SMTP Hole? (Thread)

Relevant URL:

<http://www.securityfocus.com/archive/88/344267>

13. MS event logging (Thread)

Relevant URL:

<http://www.securityfocus.com/archive/88/344108>

14. SecurityFocus Microsoft Newsletter #162 (Thread)

Relevant URL:

<http://www.securityfocus.com/archive/88/344106>

15. Allowing site redirection with URLScan (Thread)

Relevant URL:

<http://www.securityfocus.com/archive/88/344103>

16. Article Announcement: Reeducation Campaign (Thread)

Relevant URL:

<http://www.securityfocus.com/archive/88/344003>

IV. NEW PRODUCTS FOR MICROSOFT PLATFORMS

1. EnCase Enterprise Edition

By: Guidance Software Inc.

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

Relevant URL: http://www.guidancesoftware.com/frame_encase.html

Summary:

EnCase, a computer forensic tool, is Windows– based and fully integrated. A tool that allows an investigator to conduct a complete, non–invasive forensic investigation from start to finish. This tool is used by law enforcement and has been accepted and authenticated in hundreds of court cases.

2. SafeGuard PDA

By: Utimaco

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

Relevant URL: http://www.utimaco.com/content_products/sg_pda.html

Summary:

SafeGuard PDA is a powerful solution to protect your Personal Digital Assistant and the data stored on it against unauthorized access. Whether the Pocket PC is for private use or a part of the company network, it requires at least the same degree of protection as notebooks and

workstations. Since overall security is only as strong as the weakest link, SafeGuard PDA is the next logical step towards securing your mobile work force. Innovative authentication mechanisms such as biometric signature recognition or Symbol PIN offer optimal user convenience, the strong encryption protects your data while stored or in transit over the Internet, the centrally enforceable security policy keeps your environment consistently protected.

3. The CyberAngel Security Software

By: CyberAngel Security Solutions, Inc.

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

Relevant URL: <http://www.thecyberangel.com/ca-secure.html>

Summary:

The CyberAngel Security Software, a comprehensive approach to providing security for your laptop or desktop computer.

The CyberAngel Security Software utilizes our patented technology to Alert, Lock and Locate in the event of an unauthorized access of a computer.

4. Cyber-Ark Inter-Business Vault

By: Cyber-Ark

Platforms: Linux, Windows 2000, Windows NT, Windows XP

Relevant URL:

http://www.cyber-ark.com/datasecuritysoftware/inter-business_vault.htm

Summary:

Based on Cyber-Ark Software's Vaulting Technology, the Inter-Business Vault, an information security solution that enables organizations to safely overcome traditional network boundaries in order to securely share business information among customers, business partners, and remote branches. It provides a seamless, LAN-like experience over the Internet that includes all the security, performance, accessibility, and ease of administration required to allow organizations to share everyday information worldwide. To learn more about these core attributes of the Inter-Business Vault click on the relevant link below:

5. EnCase Forensic Edition

By: Guidance Software Inc.

Platforms: DOS, FreeBSD, Linux, MacOS, NetBSD, OpenBSD, PalmOS, Solaris, UNIX, Windows 2000, Windows 95/98, Windows NT, Windows XP

Relevant URL:

<http://www.guidancesoftware.com/products/EnCaseForensic/index.shtm>

Summary:

EnCase Forensic Edition Version 4 delivers the most advanced features for computer forensics and investigations. With an intuitive GUI and superior performance, EnCase Version 4 provides investigators with the tools to conduct large-scale and complex investigations with accuracy and efficiency. Guidance Software's award winning solution yields completely

non-invasive computer forensic investigations while allowing examiners to easily manage large volumes of computer evidence and view all relevant files, including "deleted" files, file slack and unallocated space.

The integrated functionality of EnCase allows the examiner to perform all functions of the computer forensic investigation process. EnCase's EnScript, a powerful macro-programming language and API included within EnCase, allows investigators to build customized and reusable forensic scripts.

6. OverflowGuard

By: DATA Security Software

Platforms: Windows 2000, Windows NT, Windows XP

Relevant URL: <http://www.datasecuritysoftware.com/index.html>

Summary:

OverflowGuard provides stack and heap buffer overflow protection for services running under Windows NT4, 2000, XP and 2003.

V. NEW TOOLS FOR MICROSOFT PLATFORMS

1. OSIRIS v2.1.0

By: The Shmoo Group

Relevant URL: <http://osiris.shmoo.com>

Platforms: BSDI, FreeBSD, Linux, MacOS, OpenBSD, UNIX, Windows 2000, Windows NT, Windows XP

Summary:

Osiris is a host integrity management system that can be used to monitor changes to a network of hosts over time and report those changes back to the administrator(s). Currently, this includes monitoring any changes to the filesystems. Osiris takes periodic snapshots of the filesystem and stores them in a database. These databases, as well as the configurations and logs, are all stored on a central management host. When changes are detected, Osiris will log these events to the system log and optionally send email to an administrator. In addition to files, Osiris has preliminary support for the monitoring of other system information including user lists, file system details, kernel modules, and network interface configurations (not included with in this beta release).

2. Glub Tech Secure FTP v2.0.11

By: glub

Relevant URL: <http://secureftp.glub.com>

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

Summary:

Glub Tech Secure FTP is a command-line utility that allows FTP connections to be made using SSL.

3. Enigmail v0.82.0

By: Patrick

Relevant URL: <http://enigmail.mozdev.org/thunderbird.html>

Platforms: Linux, MacOS, POSIX, UNIX, Windows 2000, Windows 3.x, Windows 95/98, Windows CE, Windows NT, Windows XP

Summary:

Enigmail is a "plugin" for the mail client of Mozilla and Netscape 7.x which allows users to access the authentication and encryption features provided by the popular GnuPG software. Enigmail can encrypt/sign mail when sending, and can decrypt/authenticate received mail. It can also import/export public keys. Enigmail supports both the inline PGP format and the PGP/MIME format, which can be used to encrypt attachments. Enigmail is cross-platform, although binaries are supplied only for a limited number of platforms. Enigmail uses inter-process communication to execute GPG to carry out encryption/authentication.

4. GPA (GNU Privacy Assistant) v0.7.0

By: Bernhard Reiter

Relevant URL: [http://www.gnupg.org/\(en\)/related_software/gpa/index.html](http://www.gnupg.org/(en)/related_software/gpa/index.html)

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

Summary:

The GNU Privacy Assistant is a graphical frontend to GnuPG and may be used to manage the keys and encrypt/decrypt/sign/check files. It is much like Seahorse.

5. Anti-Spam SMTP Proxy v1.0.6

By: John Hanna

Relevant URL: <http://assp.sourceforge.net/>

Platforms: BSDI, Linux, MacOS, Os Independent, OS/2, Perl (any system supporting perl), POSIX, Windows 2000, Windows NT

Summary:

The Anti-Spam SMTP Proxy (ASSP) Server project aims to create an open source platform independent SMTP Proxy server which implements whitelists and Bayesian filtering to help stop unsolicited commercial email (UCE). Anti-spam tools should be adaptive to new spam and customized for each site's email patterns. This easy to use tool works with any mail transport and achieves these goals requiring no operator intervention after the initial setup phase.

6. PipeACL tools v1.0

By: Bindview <info@razor.bindview.com>

Relevant URL:

<http://razor.bindview.com/tools/desc/pipeacltools1.0-readme.html>

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

Summary:

The PipeACL tools package contains two separate tools for viewing and configuring Win32 named pipe ACLs (Access Control Lists). The pipeacl

utility allows you to dump various settings of a named pipe, including the Owner, Group, SACLs (System access control lists), and Dacls (Discretionary access control lists). The pipeaclui utility allows you to view and apply permissions to a specified named pipe. These changes are made in the Dacls of the named pipe itself.

VI. SPONSOR INFORMATION

This Issue Sponsored by: RSA Conference 2004

Network with over 10,000 of the brightest minds in information security at the largest, most highly-anticipated industry event of the year. Don't miss RSA Conference 2004! Choose from over 200 class sessions and see demos from more than 250 industry vendors. If your job touches security, you need to be here. Learn more or register at:

http://www.securityfocus.com/sponsor/RSA_ms-secnews_031117 and use priority code SF4.

Network with over 10,000 of the brightest minds in information security at the largest, most highly-anticipated industry event of the year. Don't miss RSA Conference 2004! Choose from over 200 class sessions and see demos from more than 250 industry vendors. If your job touches security, you need to be here. Learn more or register at

http://www.securityfocus.com/sponsor/RSA_focus-ms_031027 and use priority code SF4.
