

SecurityFocus Microsoft Newsletter #266

Source: <http://www.derkeiler.com/Mailing-Lists/securityfocus/focus-ms/2005-11/0142.html>

From: Marc Fossi (mfossi_at_securityfocus.com)

Date: 11/24/05

Date: Thu, 24 Nov 2005 08:42:02 -0700 (MST)

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

SecurityFocus Microsoft Newsletter #266

Need to know what's happening on YOUR network? Symantec DeepSight Analyzer is a free service that gives you the ability to track and manage attacks. Analyzer automatically correlates attacks from various Firewall and network based Intrusion Detection Systems, giving you a comprehensive view of your computer or general network. Sign up today!

http://www.securityfocus.com/sponsor/Symantec_sf-news_041130

I. FRONT AND CENTER

1. Sony-baloney
2. Windows rootkits in 2005, part two

II. MICROSOFT VULNERABILITY SUMMARY

1. Multiple Vendor Antivirus Products Obscured File Name Scan Evasion Vulnerability
2. Apple iTunes 6 For Windows Arbitrary Local Code Execution Vulnerability
3. Multiple Vendor IpCommandLine Application Path Vulnerability
4. Floosietek FTGate IMAP Server Buffer Overflow Vulnerability
5. Oracle Database Windows XP Simple File Sharing Authentication Bypass Vulnerability
6. IBM Informix Dynamic Server Windows XP Simple File Sharing Authentication Bypass Vulnerability
7. IBM DB2 Windows XP Simple File Sharing Authentication Bypass Vulnerability
8. Counterpane Password Safe Insecure Encryption Vulnerability
9. FreeFTPD User Command Buffer Overflow Vulnerability
10. Microsoft Windows Plug and Play Denial of Service Vulnerability
11. Opera Web Browser HTML Form Status Bar Misrepresentation Vulnerability
12. FreeFTPD Multiple Buffer Overflow Vulnerabilities
13. Qualcomm Worldmail Server Directory Traversal Vulnerability
14. MailEnable IMAP Mailbox Name Buffer Overflow Vulnerability
15. Magic Winmail Server Multiple Input Validation Vulnerabilities

16. MailEnable IMAP Command Directory Traversal Vulnerability
17. Hitachi Products Multiple Cross-Site Scripting Vulnerabilities
18. Hitachi Collaboration Schedule Unspecified Denial Of Service

Vulnerability

19. Opera Web Browser Arbitrary Command Execution Vulnerability

III. MICROSOFT FOCUS LIST SUMMARY

1. ISA Server or Firewall Appliance?

IV. UNSUBSCRIBE INSTRUCTIONS

V. SPONSOR INFORMATION

I. FRONT AND CENTER

1. Sony-baloney

By Scott Granneman

The Sony story brings up dozens of questions about where we are headed with DRM issues and security, and what's really at stake.

<http://www.securityfocus.com/columnists/370>

2. Windows rootkits in 2005, part two

By James Butler, Sherri Sparks

This three-part article series looks at Windows rootkits indepth. Part two focuses on the latest cutting edge rootkit technologies that are used to hide malicious code from security scanners.

<http://www.securityfocus.com/infocus/1851>

II. MICROSOFT VULNERABILITY SUMMARY

1. Multiple Vendor Antivirus Products Obscured File Name Scan Evasion Vulnerability

BugTraq ID: 15423

Remote: Yes

Date Published: 2005-11-15

Relevant URL: <http://www.securityfocus.com/bid/15423>

Summary:

Multiple antivirus products from various vendors are reported prone to a vulnerability that may allow malicious files to bypass detection.

This issue arises when an affected application processes a file with an obscured file name.

This issue could result in malicious files bypassing detection and allowing them to be opened by a recipient.

Update: Symantec is currently investigating this issue in regards to Symantec products. It is unclear at this time if malicious files may evade scanning, or if the automatic removal feature fails. This BID will be updated as further information is disclosed.

2. Apple iTunes 6 For Windows Arbitrary Local Code Execution Vulnerability

BugTraq ID: 15446

Remote: No

Date Published: 2005-11-15

Relevant URL: <http://www.securityfocus.com/bid/15446>

Summary:

Apple iTunes 6 for Windows is prone to an arbitrary local code execution vulnerability.

This is due to a design error in which malicious code may be executed in the context of the user running the affected application.

3. Multiple Vendor IpCommandLine Application Path Vulnerability BugTraq ID: 15448

Remote: No

Date Published: 2005-11-16

Relevant URL: <http://www.securityfocus.com/bid/15448>

Summary:

Multiple vendor applications are prone to an arbitrary local code execution vulnerability.

This is due to a design error in which malicious code may be executed in the context of the user running the affected application.

4. Floosietek FTGate IMAP Server Buffer Overflow Vulnerability BugTraq ID: 15449

Remote: Yes

Date Published: 2005-11-16

Relevant URL: <http://www.securityfocus.com/bid/15449>

Summary:

Floosietek FTGate is prone to a remote buffer overflow vulnerability in the IMAP server. Successful exploitation could result in a denial of service or execution of arbitrary code.

5. Oracle Database Windows XP Simple File Sharing Authentication Bypass Vulnerability

BugTraq ID: 15450

Remote: Yes

Date Published: 2005-11-16

Relevant URL: <http://www.securityfocus.com/bid/15450>

Summary:

Oracle Database is affected by an authentication bypass vulnerability when run on Microsoft Windows XP computers that have Simple File Sharing enabled.

This vulnerability may let attackers compromise the database using the Windows XP Guest account.

The researcher who discovered this issue has not provided a conclusive list of affected Oracle database products. For the time being, all versions that run on Windows XP are assumed to be affected. If contrary information is made available, this BID will be updated accordingly.

6. IBM Informix Dynamic Server Windows XP Simple File Sharing Authentication Bypass Vulnerability

BugTraq ID: 15451

Remote: Yes

Date Published: 2005-11-16

Relevant URL: <http://www.securityfocus.com/bid/15451>

Summary:

IBM Informix Dynamic Server (IBM Informix IDS) is affected by an authentication bypass vulnerability when run on Microsoft Windows XP computers that have Simple File Sharing enabled.

This vulnerability may let attackers gain unauthorized access to the database using the Windows XP Guest account.

The researcher who discovered this issue has not provided a conclusive list of affected IBM Informix Dynamic Server products. For the time being, all versions that run on Windows XP are assumed to be affected. If contrary information is made available, this BID will be updated accordingly.

7. IBM DB2 Windows XP Simple File Sharing Authentication Bypass Vulnerability

BugTraq ID: 15452

Remote: Yes

Date Published: 2005-11-16

Relevant URL: <http://www.securityfocus.com/bid/15452>

Summary:

IBM DB2 is affected by an authentication bypass vulnerability when run on Microsoft Windows XP computers that have Simple File Sharing enabled.

This vulnerability may let attackers gain unauthorized access to the database using the Windows XP Guest account. This could be exploited with a custom client that will authenticate the attacker as the Guest account.

The researcher who discovered this issue has not provided a conclusive list of affected IBM DB2 products. For the time being, all versions that run on Windows XP are assumed to be affected. If contrary information is made available, this BID will be updated accordingly.

8. Counterpane Password Safe Insecure Encryption Vulnerability

BugTraq ID: 15455

Remote: No

Date Published: 2005-11-16

Relevant URL: <http://www.securityfocus.com/bid/15455>

Summary:

Counterpane Password Safe is susceptible to an insecure encryption vulnerability that allows easier brute force decryption attacks.

Password Safe uses a key-stretching algorithm designed to dramatically slow down brute force password guessing attacks. A random value is encrypted with the Blowfish algorithm one thousand times with a value derived from the password used as the encryption key. In order to brute force attack the Password Safe database, an attacker must follow the same one thousand encryption steps on every password guess. This is done to make brute force attacks much more time and resource intensive, lowering the likelihood of a

successful attack.

This vulnerability allows attackers with access to the Password Safe database to employ a brute force password guessing attack against the database much more efficiently than the Password Safe design intended. The data contained in the Password Safe database aids malicious users in further attacks.

9. FreeFTPD User Command Buffer Overflow Vulnerability

BugTraq ID: 15457

Remote: Yes

Date Published: 2005-11-16

Relevant URL: <http://www.securityfocus.com/bid/15457>

Summary:

freeFTPD is prone to a buffer overflow vulnerability. This issue is due to a failure in the application to do proper bounds checking on user-supplied data before storing it in a finite sized buffer.

An attacker can exploit this issue to crash the server, denying service to legitimate users. Arbitrary code execution with SYSTEM privileges may also be possible.

10. Microsoft Windows Plug and Play Denial of Service Vulnerability

BugTraq ID: 15460

Remote: Yes

Date Published: 2005-11-16

Relevant URL: <http://www.securityfocus.com/bid/15460>

Summary:

Microsoft Windows Plug and Play service is prone to a denial of service condition. This issue is caused by a malformed request to the service that causes virtual memory consumption.

On Windows XP, a remote attacker must authenticate over RPC to exploit this issue using the originally described attack vector.

Update: A reliable source has indicated that this issue is anonymously exploitable via named pipes or other MSRPC calls on Microsoft Windows XP SP2. This issue may be exploited by differing attack vectors than originally described by Microsoft.

11. Opera Web Browser HTML Form Status Bar Misrepresentation Vulnerability

BugTraq ID: 15472

Remote: Yes

Date Published: 2005-11-16

Relevant URL: <http://www.securityfocus.com/bid/15472>

Summary:

A vulnerability has been identified in Opera Web browser that allows an attacker to misrepresent the status bar in the browser, allowing vulnerable users to be misled into following a link to a malicious site.

This vulnerability would most likely be exploited through HTML e-mail, though other attack vectors exist such as HTML injection attacks in third-party Web

applications.

12. FreeFTPD Multiple Buffer Overflow Vulnerabilities

BugTraq ID: 15486

Remote: Yes

Date Published: 2005-11-17

Relevant URL: <http://www.securityfocus.com/bid/15486>

Summary:

freeFTPd is prone to multiple buffer overflow vulnerabilities. These issues are due to a failure in the application to do proper bounds checking on user-supplied data before storing it in finite sized buffers.

An attacker can exploit these issues to crash the server, denying service to legitimate users. Arbitrary code execution with SYSTEM privileges may also be possible.

13. Qualcomm Worldmail Server Directory Traversal Vulnerability

BugTraq ID: 15488

Remote: Yes

Date Published: 2005-11-17

Relevant URL: <http://www.securityfocus.com/bid/15488>

Summary:

Qualcomm Worldmail server is prone to a directory traversal vulnerability. Successful exploitation could allow an attacker to gain access to files owned by other users of the application.

Sensitive information may be obtained and modified in this manner.

Worldmail server version 3.0 is vulnerable; other versions may also be affected.

14. MailEnable IMAP Mailbox Name Buffer Overflow Vulnerability

BugTraq ID: 15492

Remote: Yes

Date Published: 2005-11-18

Relevant URL: <http://www.securityfocus.com/bid/15492>

Summary:

MailEnable is prone to a buffer overflow vulnerability in multiple IMAP commands. The issue is due to improper bounds checking on the mailbox name argument supplied to various commands.

This issue is reported to affect MailEnable Professional 1.6 with Hotfix MEIMAPS-UPD0511010000.zip and MailEnable Enterprise 1.1 with Hotfix MEIMAPS-UPD0511010000.zip. Other versions may also be vulnerable.

15. Magic Winmail Server Multiple Input Validation Vulnerabilities

BugTraq ID: 15493

Remote: Yes

Date Published: 2005-11-18

Relevant URL: <http://www.securityfocus.com/bid/15493>

Summary:

Magic Winmail Server is prone to multiple input validation vulnerabilities.

These issues are due to a failure in the application to properly sanitize user-supplied input.

Magic Winmail Server is prone to cross-site scripting, HTML injection and directory traversal vulnerabilities.

16. MailEnable IMAP Command Directory Traversal Vulnerability

BugTraq ID: 15494

Remote: Yes

Date Published: 2005-11-18

Relevant URL: <http://www.securityfocus.com/bid/15494>

Summary:

MailEnable is prone to a directory traversal vulnerability when processing certain IMAP commands. Successful exploitation could allow data corruption.

This issue is reported to affect MailEnable Professional 1.6 with Hotfix MEIMAPS-UPD0511010000.zip and MailEnable Enterprise 1.1 with Hotfix MEIMAPS-UPD0511010000.zip. Other versions may also be vulnerable.

17. Hitachi Products Multiple Cross-Site Scripting Vulnerabilities

BugTraq ID: 15498

Remote: Yes

Date Published: 2005-11-18

Relevant URL: <http://www.securityfocus.com/bid/15498>

Summary:

Hitachi Collaboration Schedule and Collaboration Calendar are prone to multiple unspecified cross-site scripting vulnerabilities. These are due to a lack of proper sanitization of user-supplied input.

An attacker may leverage these issues to have arbitrary script code executed in the browser of an unsuspecting user in the context of the affected site. These may facilitate the theft of cookie-based authentication credentials as well as other attacks.

18. Hitachi Collaboration Schedule Unspecified Denial Of Service Vulnerability

BugTraq ID: 15500

Remote: Yes

Date Published: 2005-11-18

Relevant URL: <http://www.securityfocus.com/bid/15500>

Summary:

Hitachi Collaboration Schedule is prone to a denial of service vulnerability.

This vulnerability may be triggered by multiple invalid requests sent to the schedule.

No further details have been provided.

19. Opera Web Browser Arbitrary Command Execution Vulnerability

BugTraq ID: 15521

Remote: Yes

Date Published: 2005-11-22

Relevant URL: <http://www.securityfocus.com/bid/15521>

Summary:

Opera Web Browser is affected by an arbitrary command execution vulnerability.

User-supplied data passed through a URI is not properly sanitized, allowing an attacker to use a specially crafted URI and enticing a user to follow it to execute arbitrary commands through the shell.

This attack may facilitate unauthorized remote access.

Opera 8.50 and prior versions running on Unix and Linux platforms are vulnerable to this issue. This vulnerability is identical to BID 14888 (Mozilla Browser/Firefox Arbitrary Command Execution Vulnerability).

III. MICROSOFT FOCUS LIST SUMMARY

1. ISA Server or Firewall Appliance?

<http://www.securityfocus.com/archive/88/416700>

IV. UNSUBSCRIBE INSTRUCTIONS

To unsubscribe send an e-mail message to ms-secnews-unsubscribe@securityfocus.com from the subscribed address. The contents of the subject or message body do not matter. You will receive a confirmation request message to which you will have to answer. Alternatively you can also visit <http://www.securityfocus.com/newsletters> and unsubscribe via the website.

If your email address has changed email listadmin@securityfocus.com and ask to be manually removed.

V. SPONSOR INFORMATION

Need to know what's happening on YOUR network? Symantec DeepSight Analyzer is a free service that gives you the ability to track and manage attacks. Analyzer automatically correlates attacks from various Firewall and network based Intrusion Detection Systems, giving you a comprehensive view of your computer or general network. Sign up today!

http://www.securityfocus.com/sponsor/Symantec_sf-news_041130
