

# SecurityFocus Microsoft Newsletter #154

**Source:** <http://www.derkeiler.com/Mailing-Lists/securityfocus/focus-ms/2003-09/0092.html>

---

**From:** Marc Fossi (*mfossi\_at\_securityfocus.com*)

**Date:** 09/16/03

Date: Tue, 16 Sep 2003 07:05:05 -0600 (MDT)

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

SecurityFocus Microsoft Newsletter #154

---

This Issue is Sponsored by: SecurityFocus

We are pleased to announce the launch of two new mailing lists for the Security community:

1. Security Management ([security-management-subscribe@securityfocus.com](mailto:security-management-subscribe@securityfocus.com))
2. Bugtraq-French ([bugtraq-french-subscribe@securityfocus.com](mailto:bugtraq-french-subscribe@securityfocus.com))

To subscribe to either of these lists, send mail to the listserv at the respective address indicated above; the subject and body of your message do not matter. Or, you can visit our signup page at

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

---

## I. FRONT AND CENTER

1. Dynamic Honeypots
2. Demonstrating ROI for Penetration Testing (Part Three)
3. Hardening the TCP/IP stack to SYN attacks
4. SecurityFocus New Mailing List Announcement

## II. MICROSOFT VULNERABILITY SUMMARY

1. FoxWeb PATH\_INFO Remote Buffer Overrun Vulnerability
2. ISS RealSecure Server Sensor SSL Denial Of Service Vulnerabi...
3. Microsoft Internet Explorer Browser Popup Window Object Type...
4. Microsoft ASP.NET Request Validation Null Byte Filter Bypass...
5. ICQ Webfront guestbook Cross-Site Scripting Vulnerability
6. Kukol E.V. HTTP & FTP Server Suite File Disclosure Vulnerabi...
7. Microsoft Internet Explorer XML Page Object Type Validation ...
8. Roger Wilco Remote Server Side Buffer Overrun Vulnerability
9. NullSoft Winamp MIDI Plugin IN\_MIDI.DLL Track Data Size Buff...
10. Roger Wilco Remote Username Denial of Service Vulnerability
11. PHPBB URL BBCode HTML Injection Vulnerability
12. RealOne Player Insecure Configuration File Permission Local ...
13. WinRAR Compressed File Size Misrepresentation Weakness
14. Invision Power Board Index.php Showtopic Cross-Site Scriptin...
15. Multiple Microsoft Internet Explorer Script Execution Vulner...

16. Yak! Chat Client FTP Server Default Credentials Vulnerabilit...
17. KokeshCMS Unauthorized Content Editing Vulnerability
18. Pine Message/External–Body Type Attribute Buffer Overflow Vu...
19. MySQL Password Handler Buffer Overflow Vulnerability

### III. MICROSOFT FOCUS LIST SUMMARY

1. windows 2000 security logs (Thread)
2. Disabling sharing and group policies (Thread)
3. Security for Win XP Home (Thread)
4. GPO for one machine (Thread)
5. RE: Disabling sharing and group policies (Thread)
6. Domain vs. Local security policy (Thread)
7. Disable USB on a per user basis? (Thread)
8. Limiting users on secific machines that are part of ... (Thread)
9. Voting on issues for this list and SecurityFocus (Fo... (Thread)
10. SecurityFocus Microsoft Newsletter #153 (Thread)
11. Possible information leakage from DNS quirks (Thread)
12. SecurityFocus Microsoft Newsletter #152 (Thread)

### IV. NEW PRODUCTS FOR MICROSOFT PLATFORMS

1. Sophos Anti–Virus
2. LANDesk Management Suite 7
3. McAfee ePolicy Orchestrator
4. Enterprise Manager
5. ZoneAlarm Pro 4.0
6. ActiveScout Enterprise

### V. NEW TOOLS FOR MICROSOFT PLATFORMS

1. The OpenAntivirus Project: Summary Various
2. BO2K v1.1.1
3. OSIRIS v2.0.0b
4. SysOrb v2.4.2
5. ccrypt v1.6
6. Star v1.5a21

### VI. SPONSOR INFORMATION

#### I. FRONT AND CENTER

---

1. Dynamic Honeypots  
By Lance Spitzner

The search for the dream honeypot: dynamic honeypots, an appliance–like plug–and–play solution.

<http://www.securityfocus.com/infocus/1731>

2. Demonstrating ROI for Penetration Testing (Part Three)  
By Marcia Wilson

The third article in this series focuses on defining terms related to the Risk Analysis process and touches on Information Asset valuation methods that are critical when justifying the necessity and expense of a Pen Test.

<http://www.securityfocus.com/infocus/1730>

### 3. Hardening the TCP/IP stack to SYN attacks

By Mariusz Burdach

This article discusses methods of hardening the TCP/IP stack of various operating systems to make servers more resistant to SYN flooding and SYN spoofing Denial of Service (DOS) attacks.

<http://www.securityfocus.com/infocus/1729>

### 4. SecurityFocus New Mailing List Announcement

We are pleased to announce the launch of two new mailing lists for the Security community:

1. Security Management ([security-management-subscribe@securityfocus.com](mailto:security-management-subscribe@securityfocus.com))
2. Bugtraq-French ([bugtraq-french-subscribe@securityfocus.com](mailto:bugtraq-french-subscribe@securityfocus.com))

To subscribe to either of these lists, send mail to the listserv at the respective address indicated above; the subject and body of your message do not matter. Or, you can visit our signup page at

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

## II. MICROSOFT VULNERABILITY SUMMARY

---

### 1. FoxWeb PATH\_INFO Remote Buffer Overrun Vulnerability

BugTraq ID: 8547

Remote: Yes

Date Published: Sep 05 2003

Relevant URL: <http://www.securityfocus.com/bid/8547>

Summary:

FoxWeb is a Foxpro-based web application development framework. It is available for Microsoft Windows operating systems.

FoxWeb is prone to a remotely exploitable buffer overrun vulnerability. This is due to insufficient bounds checking of user-supplied PATH\_INFO data to the FoxWeb CGI and ISAPI extension (foxweb.exe and foxweb.dll). If more than 3000 bytes are supplied as input to PATH\_INFO, adjacent regions of stack memory may be overrun with the excessive data. This could potentially allow a remote attacker to corrupt stack variables, such as a return address, with specific data. This may be leveraged by the attacker to control the execution flow of the program.

Successful exploitation would permit a remote attacker to execute arbitrary code in the context of the software.

### 2. ISS RealSecure Server Sensor SSL Denial Of Service Vulnerabi...

BugTraq ID: 8550

Remote: Yes

Date Published: Sep 05 2003

Relevant URL: <http://www.securityfocus.com/bid/8550>

Summary:

ISS RealSecure Server Sensor is an intrusion detection technology that can integrate with an underlying web server such as Microsoft IIS or Apache. It supports a number of platforms including Microsoft Windows and Unix/Linux variants.

ISS RealSecure Server Sensor is prone to a denial of service when handling a malicious request over SSL. It is reportedly possible to reproduce this condition by passing invalid unicode characters in a request over SSL. This vulnerability could be exploited to crash the underlying Microsoft IIS web server. It should be noted that the service may be automatically restarted.

It is not known if this issue affects other platforms or can be exploited to crash other underlying web server implementations.

The researchers who discovered this vulnerability are currently investigating the possibility of exploiting this issue to execute arbitrary code, though sufficient details are not available regarding this at the time of writing. This BID will be updated and impacts adjusted accordingly if more details become available.

### 3. Microsoft Internet Explorer Browser Popup Window Object Type...

BugTraq ID: 8556

Remote: Yes

Date Published: Sep 07 2003

Relevant URL: <http://www.securityfocus.com/bid/8556>

Summary:

Internet Explorer does not properly handle object types, when rendering web browser popup windows. This may result in the possibility of the execution of malicious software.

The problem occurs when Internet Explorer receives a response from the server when a malicious popup window containing an object tag is parsed. Proper parameter checks of the type of file being loaded are not performed on the object type contained within HTTP response received from the web server.

Successful exploitation of this vulnerability could allow a malicious object to be trusted and as such be installed and executed on the local system. All code execution would occur in the security context of the user running the affected browser. It should be noted that an attacker might be capable of also executing locally installed executables with command-line parameters.

This issue is related to Microsoft Bulletin MS03-032 and BID 8456, it has also been reported to be related to BID 3867.

### 4. Microsoft ASP.NET Request Validation Null Byte Filter Bypass...

BugTraq ID: 8562

Remote: Yes

Date Published: Sep 08 2003

Relevant URL: <http://www.securityfocus.com/bid/8562>

Summary:

ASP.NET 1.1 ships with a Request Validation feature that is designed to sanitize malicious user-supplied HTML before it is rendered to clients.

It has been reported that Request Validation does not perform as expected, and under some circumstances may be bypassed. As a result, ASP scripts that depend on Request Validation to sanitize user-supplied input may still be prone to cross-site scripting or HTML injection attacks as a result. Request Validation may be bypassed by including a null byte (%00) in malicious user-supplied input. It has been demonstrated that this issue may be exploited if a null byte is placed after the '<' character in a HTML tag, for example:

```
<%00script>
```

This will effectively bypass the feature, but many clients will ignore the null byte and render the HTML tag normally.

It should be noted that this can also create a false sense of security, since the expectation is that Request Validation should sufficiently sanitize hostile input. Developers may design scripts with this expectation and not implement native validation of user-supplied input.

#### 5. ICQ Webfront guestbook Cross-Site Scripting Vulnerability

BugTraq ID: 8563

Remote: Yes

Date Published: Sep 08 2003

Relevant URL: <http://www.securityfocus.com/bid/8563>

Summary:

ICQ is an instant messenger client for Microsoft Windows systems and other platforms. ICQ Webfront is used to create personal web sites that are integrated with a user's ICQ client. ICQ Webfront allows users to share personal information, contacts, and files with other users.

A vulnerability has been reported to exist in the message field of the guestbook module of ICQ Webfront. This issue may allow a remote attacker to execute HTML or script code in a user's browser due to insufficient sanitization of user input.

The problem is reported to exist due to a lack of sanitization of user-supplied input by the software. HTML and script code will be rendered in a user's browser, therefore making it possible for an attacker to construct a malicious link containing HTML or script code that may be rendered in a user's browser upon visiting that link. This attack would occur in the security context of the affected site.

Successful exploitation of this vulnerability may allow an attacker to steal cookie-based authentication credentials. Other attacks may well be

possible.

ICQ 2003 has been listed as a vulnerable package, however other versions may be affected as well.

6. Kukol E.V. HTTP & FTP Server Suite File Disclosure Vulnerabi...

BugTraq ID: 8564

Remote: Yes

Date Published: Sep 08 2003

Relevant URL: <http://www.securityfocus.com/bid/8564>

Summary:

Kukol E.V. HTTP & FTP Server Suite is a web/file server that is available for Microsoft Windows operating systems.

The web server component of Kukol E.V. HTTP & FTP Server Suite is prone to a file disclosure vulnerability. Remote web users may use directory traversal sequences in requests to gain access to files outside of the server's web root directory. In this manner, contents of files that are readable by the web server may be disclosed to remote attackers.

This vulnerability has the potential to disclose sensitive information that may be useful in mounting further attacks against the system hosting the software.

7. Microsoft Internet Explorer XML Page Object Type Validation ...

BugTraq ID: 8565

Remote: Yes

Date Published: Sep 08 2003

Relevant URL: <http://www.securityfocus.com/bid/8565>

Summary:

Internet Explorer does not properly handle object types, when rendering XML based web sites. This may result in the possibility of the execution of malicious software.

The problem occurs when Internet Explorer receives a response from the server when a malicious XML web page containing an embedded object tag is parsed. Proper parameter checks of the type of file being loaded are not performed on the object type contained within HTTP response received from the web server.

Successful exploitation of this vulnerability could allow a malicious object to be trusted and as such be installed and executed on the local system. All code execution would occur in the security context of the user running the affected browser. It should be noted that an attacker might be capable of also executing locally installed executables with command-line parameters.

This issue is related to Microsoft Bulletin MS03-032, BID 8456 and BID 8556 it has also been reported to be related to BID 3867.

#### 8. Roger Wilco Remote Server Side Buffer Overrun Vulnerability

BugTraq ID: 8566

Remote: Yes

Date Published: Sep 08 2003

Relevant URL: <http://www.securityfocus.com/bid/8566>

Summary:

Roger Wilco is a net-based communication client designed to allow users to speak in real-time. Multiple clients may connect to a single server allowing remote users to interact. It is available for the Microsoft Windows operating servers.

A remote buffer overrun has been reported for various Roger Wilco server releases. The problem lies in the fact that the vulnerable servers rely on client-side size values when copying data into internal memory buffers.

When a client attempts to connect to a server, it first transmits a packet containing a variety of data, including the password and channel. The 3rd and 4th bytes of this packet denote the size of this data. Upon receiving this transmission, the server uses the client-supplied size value when copying the data into an internal memory buffer. As the size value is two bytes, an attacker could theoretically supply up to 65535 bytes of data to be copied into the server. As the server has previously allocated a buffer believed to be of sufficient size, this could result in a buffer overrun.

An attacker may be capable of exploiting this issue to overwrite sensitive memory variables within the server process space. This could ultimately allow for the execution flow of the server to be controlled, and may result in the execution of attacker-supplied instructions.

#### 9. NullSoft Winamp MIDI Plugin IN\_MIDI.DLL Track Data Size Buff...

BugTraq ID: 8567

Remote: Yes

Date Published: Sep 08 2003

Relevant URL: <http://www.securityfocus.com/bid/8567>

Summary:

NullSoft Winamp is a freely available media player from Nullsoft. It is available for the Microsoft Windows platform. IN\_MIDI.DLL is the default MIDI plugin used by Winamp when processing MIDI files.

Winamp MIDI plugin, IN\_MIDI.DLL has been reported prone to a buffer overflow issue when handling malicious MIDI files. The issue presents itself when a value of 'fffffff', is passed as a value for the Track Data Size of a MIDI file header. Although unconfirmed the vulnerability may be due to an unsigned signed mismatch when performing bounds checking on data that is being copied into an internal buffer in stack based memory. The signed value of 0xffffffff (-1), instead of the unsigned value may be used erroneously in boundary conditions arithmetic.

Although unconfirmed it has been conjectured that an attacker may exploit this condition to execute arbitrary code in the context of the user who is running the affected Winamp player.

It has been reported that user interaction may hinder exploitation of this vulnerability, for example how the file is opened, or the default MIDI device that is used.

It should be noted that due to default MIDI file player registry settings made when Winamp is installed, this issue may also be automatically exploitable when malicious web pages or HTML email are viewed.

Winamp version  $\geq 3.01$  IN\_MIDI.DLL has been reported prone to this issue.

#### 10. Roger Wilco Remote Username Denial of Service Vulnerability

BugTraq ID: 8568

Remote: Yes

Date Published: Sep 08 2003

Relevant URL: <http://www.securityfocus.com/bid/8568>

Summary:

Roger Wilco is a net-based communication client designed to allow users to speak in real-time. Multiple clients may connect to a single Roger Wilco server, allowing remote users to interact. It is available for the Microsoft Windows operating servers.

It has been reported that connecting to a Roger Wilco server with a username of excessive length may cause the server to crash. The problem is said to occur within the NETWORK.DLL library, specifically when someone with a 33 byte or larger username connects to the server. This may effectively deny service to other legitimate users.

Although it has not been confirmed, this issue may be due to insufficient bounds checking before copying username data into an internal memory buffer.

This vulnerability is said to affect Roger Wilco 1.4.1.6.

#### 11. PHPBB URL BBCode HTML Injection Vulnerability

BugTraq ID: 8570

Remote: Yes

Date Published: Sep 08 2003

Relevant URL: <http://www.securityfocus.com/bid/8570>

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.

BBCode is a basic restricted implementation of HTML that is used to control the appearance of text in user-supplied phpBB entries.

phpBB BBCode has been reported prone to an HTML injection vulnerability. It has been reported that an attacker may inject malicious script into areas of phpBB where BBCode is rendered, for example bulletin board posts or private messages. This issue is due to a lack of sufficient sanitization performed on user supplied URL BBCode tags. The [url] BBCode

tag is reported vulnerable.

As a result of the lack of sanitization, injected code may be rendered in the web browser of a user who views vulnerable areas of the site. This would occur in the security context of the site hosting phpBB and its related modules.

An attacker may exploit this issue to steal cookie-based authentication credentials, other attacks may also be possible.

Although this vulnerability has been reported to affect phpBB version 2.0.6, other versions may also be vulnerable.

#### 12. RealOne Player Insecure Configuration File Permission Local ...

BugTraq ID: 8571

Remote: No

Date Published: Sep 09 2003

Relevant URL: <http://www.securityfocus.com/bid/8571>

Summary:

RealOne Player is a media player that is available for a number of platforms including Microsoft Windows and MacOS systems.

RealOne Player reported prone to a local privilege escalation vulnerability.

The configuration files for the RealOne Player are installed in the '.realnetworks' hidden folder in a users home directory. The issue presents itself, because configuration files stored in this directory are installed with 0660 permissions. This means that an attacker, who is in the same group as a target user, may modify RealOne Player configuration files and may thereby escalate privileges to that of the target user.

A local attacker may exploit this condition; by creating a Trojan shared library and modifying the 'dt\_codecs' variable in the 'RealShared\_0\_0' configuration file, so that it points to the malicious shared library. This may result in arbitrary code execution in the context of the target user, when RealOne Player is executed. Other methods of exploitation are also possible.

It should be noted, that this vulnerability has been reported to affect X86 Linux variants of RealOne Player.

#### 13. WinRAR Compressed File Size Misrepresentation Weakness

BugTraq ID: 8572

Remote: Yes

Date Published: Sep 09 2003

Relevant URL: <http://www.securityfocus.com/bid/8572>

Summary:

WinRAR is a compression utility capable of reading and writing files using several different archival formats. It is available for the Microsoft Windows Operating system.

WinRAR is prone to a weakness that may allow malicious parties to misrepresent the size of compressed files. This issue occurs because WinRAR trusts values in the .rar header without adequately verifying the actual file size.

If the .rar header is otherwise correct and contains a valid CRC checksum, then WinRAR will pre-allocate space to decompress the file based on file size information provided in the header. During pre-allocation, WinRAR will not verify that there is enough disk space to decompress files included in the archive based on their actual size (since pre-allocation is based on the size specified in the header). This presents a security threat because a user may expect that a compressed file is a certain size and decompress it based on this assumption. A deceptively large file could be included in an archive that consumes all available disk space when it is decompressed. Furthermore, under some circumstances, WinRAR may attempt to extract a file based on the size specified in the header, even if the actual file size is relatively small, filling any disk space beyond the end of the decompressed file with zeroes.

UnRar, a Rar add-on distributed by RARLAB, is also prone to this issue. The UnRar add-on is available for a number of operating systems, including Unix/Linux derivatives and may be invoked automatically by various virus scanners. This could pose an additional attack vector which does not require user interaction to exploit.

There have been conflicting reports as to whether WinRAR 3.20 is vulnerable to this issue or not.

#### 14. Invision Power Board Index.php Showtopic Cross-Site Scriptin...

BugTraq ID: 8575

Remote: Yes

Date Published: Sep 09 2003

Relevant URL: <http://www.securityfocus.com/bid/8575>

Summary:

Invision Board is web forum software. It is implemented in PHP and is available for Unix and Linux variants and Microsoft Windows operating systems.

Invision Power Board index.php script reported prone to a cross-site scripting vulnerability.

The issue presents itself due to a lack of sufficient sanitization performed by functions in the index.php script on user-influenced 'showtopic' URI parameter. It has been reported that a remote attacker may construct a malicious link to the script and supply arbitrary HTML code as a value for the 'showtopic' URI parameter. If this link is followed, the content of the 'showtopic' parameter will be rendered in the browser of the user who followed the link.

This could permit the theft of cookie authentication credentials; other attacks may also be possible.

15. Multiple Microsoft Internet Explorer Script Execution Vulner...

BugTraq ID: 8577

Remote: Yes

Date Published: Sep 10 2003

Relevant URL: <http://www.securityfocus.com/bid/8577>

Summary:

Multiple issues have been reported in Microsoft Internet Explorer. Though these issues have been reported by a reliable source, communication issues have presented difficulty in obtaining details surrounding the reported issues. This vulnerability entry will be updated when additional information becomes available.

The following issues may exist, based on the limited information currently available:

1. A javascript-protocol URL left in browser history will result in the execution of javascript if the browser back button is pressed.
2. Under some circumstances, it may be possible to break functionality in Internet Explorer to map the find function to the execution of arbitrary functions. This appears to be done by hijacking the Control-F function within IE.
3. It may be possible to hijack the click function within Internet Explorer to instead perform a dragAndDrop function. By doing so, an attacker could drag an arbitrary homepage into a targeted list.
4. Similar to the issue described under point three, it may be possible to hijack a different method to perform specific actions within the browser, thus removing the need for user action to perform potentially malicious functions.
5. Due to insecure handling of script code by the search function, it is possible to execute script code in the search window. This may result in a violation of browser security policy.
6. It may be possible to bypass the URL check performed by the search method, making it possible to pass a HREF property into a BASE tag.
7. It is possible to abuse the file: protocol to potentially execute code in the local security zone. The window.external.NavigateAndFind is a method that may be abused in such an instance. This issue, combined with a previously disclosed problem, can permit an attacker to inject malicious code into the media sidebar error page, resulting in the execution of code in the security context of the "My Computer" zone.

Other issues exist, however preliminary details are either unclear or not available at this time. Further, the available information may change as available details are further clarified. This vulnerability will be further updated as more information becomes available.

16. Yak! Chat Client FTP Server Default Credentials Vulnerabilit...

BugTraq ID: 8581

Remote: Yes

Date Published: Sep 10 2003

Relevant URL: <http://www.securityfocus.com/bid/8581>

Summary:

Yak! is a commercially-available chat client distributed by Digicraft Software. It is available for the Microsoft Windows platform.

It has been reported that a vulnerability exists in the Yak! client client FTP server. This problem may allow an attacker unauthorized access to resources.

The problem is in the default credentials created with the Yak! FTP server. When the FTP server is installed, it installs a user 'Yak' with the password 'asd123' by default. This user is granted full access to the file system on which the FTP server resides. The FTP server listens on port 3535.

17. KokeshCMS Unauthorized Content Editing Vulnerability

BugTraq ID: 8585

Remote: Yes

Date Published: Sep 09 2003

Relevant URL: <http://www.securityfocus.com/bid/8585>

Summary:

KokeshCMS is a content management system that is implemented in PHP. It is available for Microsoft Windows operating systems and Unix/Linux variants.

KokeshCMS does not adequately secure access to the content editing script (edit.php). The source of the problem is that KokeshCMS does not force users to authenticate before granting access to the script. As a result, remote users can access this script without needing to authenticate. A remote attacker could exploit this issue to manipulate content on sites managed by the software, for example, placing malicious or abusive content on a site. This could pose an additional risk if users trust the site's content.

18. Pine Message/External-Body Type Attribute Buffer Overflow Vu...

BugTraq ID: 8588

Remote: Yes

Date Published: Sep 10 2003

Relevant URL: <http://www.securityfocus.com/bid/8588>

Summary:

Pine is a freely available, open source Mail User Agent. It is distributed by the University of Washington, and available for the Unix, Linux, and Microsoft platforms.

A problem in Pine has been reported when handling "message/external body type" attributes. Because of this, an attacker may be able to gain unauthorized access to a host using the vulnerable software.

The problem is in the parsing of the name/value pairs. Due to improper bounds checking, it is possible to supply a value in this field that results in the overwriting of sensitive process memory. An attacker can exploit this with a custom string to execute arbitrary code with the privileges of the Pine user.

#### 19. MySQL Password Handler Buffer Overflow Vulnerability

BugTraq ID: 8590

Remote: Yes

Date Published: Sep 10 2003

Relevant URL: <http://www.securityfocus.com/bid/8590>

Summary:

MySQL is an open source relational database project. It is available for the Microsoft Windows, Linux, and Unix operating systems.

MySQL server has been reported prone to a buffer overflow vulnerability when handling user passwords of excessive size.

The issue presents itself, due to a lack of sufficient bounds checking performed on MySQL user passwords that are stored in the 'Password' field of the 'User' table in a MySQL database. It has been reported that MySQL fails to properly perform bounds checking when processing passwords. A password greater than 16 characters may overrun the bounds of a reserved buffer in memory and corrupt adjacent memory. The buffer overflow occurs in an ACL\_USER instance of `acl_init()`, and may ultimately result in the corruption of a saved instruction pointer.

An attacker with global administrative privileges on an affected MySQL server may potentially exploit this condition to have arbitrary supplied instructions executed in the context of the MySQL server.

This vulnerability has been reported to affect all versions of MySQL up to and including 4.0.14 and 3.0.57.

### III. MICROSOFT FOCUS LIST SUMMARY

---

#### 1. windows 2000 security logs (Thread)

Relevant URL:

<http://www.securityfocus.com/archive/88/337444>

#### 2. Disabling sharing and group policies (Thread)

Relevant URL:

<http://www.securityfocus.com/archive/88/337441>

#### 3. Security for Win XP Home (Thread)

Relevant URL:

<http://www.securityfocus.com/archive/88/337312>

4. GPO for one machine (Thread)

Relevant URL:

<http://www.securityfocus.com/archive/88/337289>

5. RE: Disabling sharing and group policies (Thread)

Relevant URL:

<http://www.securityfocus.com/archive/88/337182>

6. Domain vs. Local security policy (Thread)

Relevant URL:

<http://www.securityfocus.com/archive/88/336996>

7. Disable USB on a per user basis? (Thread)

Relevant URL:

<http://www.securityfocus.com/archive/88/336930>

8. Limiting users on specific machines that are part of ... (Thread)

Relevant URL:

<http://www.securityfocus.com/archive/88/336813>

9. Voting on issues for this list and SecurityFocus (Fo... (Thread)

Relevant URL:

<http://www.securityfocus.com/archive/88/336810>

10. SecurityFocus Microsoft Newsletter #153 (Thread)

Relevant URL:

<http://www.securityfocus.com/archive/88/336759>

11. Possible information leakage from DNS quirks (Thread)

Relevant URL:

<http://www.securityfocus.com/archive/88/336536>

12. SecurityFocus Microsoft Newsletter #152 (Thread)

Relevant URL:

<http://www.securityfocus.com/archive/88/336508>

#### IV. NEW PRODUCTS FOR MICROSOFT PLATFORMS

---

1. Sophos Anti-Virus

By: Sophos

Platforms: AIX, DOS, FreeBSD, HP-UX, Linux, MacOS, Netware, OS/2, Solaris, UNIX, VMS, Windows 3.x, Windows 95/98, Windows NT

Relevant URL: <http://www.sophos.com/products/sav/>

Summary:

Sophos Anti-Virus is a unique solution to the virus problem, providing true cross-platform protection in a single, fully integrated product. The network-centric design provides a host of benefits for the protection of servers, workstations and portables. Sophos's ground-breaking architecture maximises protection, while minimising performance and administrative overheads.

## 2. LANDesk Management Suite 7

By: LANDesk Software

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

Relevant URL: <http://www.landesk.com/products/ilms/>

Summary:

LANDesk Management Suite 7 is a comprehensive, integrated management solution that's easy to use. Enabling proactive management of desktops, server and mobile devices across heterogeneous IT environments.

- Keep up with security patches and virus updates
- Efficiently install and maintain software on the desktop
- Decrease software license costs and respond to audits
- Reduce the cost of helpdesk support
- Discover and manage hardware and software assets
- Migrate many users and their profiles to new operating systems

## 3. McAfee ePolicy Orchestrator

By: Network Associates

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

Relevant URL:

<http://www.nai.com/us/products/mcafee/antivirus/fileserver/epo.htm>

Summary:

McAfee Security ePolicy Orchestrator (ePO) is the market-leading tool for centralized policy management of malicious threat protection. ePO allows you to maintain up-to-date protection, configure and enforce policies, and generate detailed graphical reports on McAfee Security and third party products, including Symantec and Dr Ahn anti-virus products.

## 4. Enterprise Manager

By: Sophos

Platforms: Windows 2000, Windows NT

Relevant URL: <http://www.sophos.com/products/em/>

Summary:

The Enterprise Manager suite is a powerful set of tools allowing fully automated web-based installation and updating of Sophos software across a network and even to remote users.

Network administrators are put in full control and can monitor their network at all times. Unprotected computers or those running an out-of-date version of Sophos Anti-Virus can be immediately and automatically updated. In practice, a network of 1000 or more clients can be updated from a single, central Windows machine within five minutes.

#### 5. ZoneAlarm Pro 4.0

By: Zone Labs

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

Relevant URL: <http://www.zonelabs.com>

Summary:

Hackers lurk everywhere on the Internet, waiting for an "in" into your personal and financial information. Even legitimate Web sites have sophisticated methods of snooping, such as cookies that track your identity and browsing habits. You need nothing less than the industry's best protection?ZoneAlarm Pro. It offers you the award-winning firewall that Zone Labs is famous for. Plus, it stops annoying and potentially malicious cookies and pop-ups from invading your system.

#### 6. ActiveScout Enterprise

By: ForeScout Technologies

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

Relevant URL: <http://www.forescout.com/enterprise.html>

Summary:

ActiveScout Enterprises actively protects a network with multiple access points. In addition to the identification of attackers and automatic action to stop them, this solution offers full management capabilities, from configuration and reporting, to the sharing of threat information between multiple deployed scouts.

### V. NEW TOOLS FOR MICROSOFT PLATFORMS

---

#### 1. The OpenAntivirus Project: Summary Various

By: cbricart, fz-net, hfuhs, kurti and reniar

Relevant URL: <http://www.openantivirus.org/>

Platforms: Os Independent, POSIX, Windows 2000, Windows 95/98, Windows NT, Windows XP

Summary:

Developing Open Source AntiVirus Solutions

#### 2. BO2K v1.1.1

By: andrereis and j\_aroche

Relevant URL: <http://www.bo2k.com/>

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

Summary:

BO2K is a remote administration tool for Windows systems. It comes with a client and a server. The server is lightweight and inobtrusive. A dynamic

plugin architecture allows for easy system extension.

### 3. OSIRIS v2.0.0b

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).

### 4. SysOrb v2.4.2

By: oestergaard

Relevant URL: <http://www.sysorb.com/>

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

Summary:

SysOrb is a client/server package that can monitor servers remotely (such as Web servers), or monitor devices on servers (such as disks, memory, load, etc.). It will alert the administrators via e-mail or pager if a server is entering a critical condition, and has its own database backend, allowing for massive collection of system statistics.

### 5. ccrypt v1.6

By: Peter Selinger

Relevant URL: <http://quasar.mathstat.uottawa.ca/~selinger/ccrypt/>

Platforms: AIX, FreeBSD, Linux, MacOS, Solaris, SunOS, Windows 2000, Windows 95/98, Windows NT

Summary:

ccrypt is a commandline utility for encrypting and decrypting files and streams. It was designed as a replacement for the standard Unix crypt utility, which is notorious for using a very weak encryption algorithm. ccrypt is based on the Rijndael cipher, which is the U.S. government's chosen candidate for the Advanced Encryption Standard (AES). This cipher is believed to provide very strong security. A compatibility mode is included for decrypting legacy "unix crypt" files.

### 6. Star v1.5a21

By: Jörg Schilling

Relevant URL:

<http://www.fokus.gmd.de/research/cc/gclone/employees/joerg.schilling/private/star.html>

Platforms: BeOS, MacOS, OS/2, POSIX, Windows 2000, Windows 95/98, Windows NT, Windows XP

Summary:

Star is a very fast, POSIX-compliant tar archiver. It reads and writes POSIX compliant tar archives as well as non-POSIX GNU tar archives. Star is the first free POSIX.1-2001 compliant tar implementation. It saves many files together into a single tape or disk archive, and can restore individual files from the archive. It includes a FIFO for speed, a pattern matcher, multi-volume support, the ability to archive sparse files and ACLs, the ability to archive extended file flags, automatic archive format detection, automatic byte order recognition, automatic archive compression/decompression, remote archives, and special features that allow star to be used for full and incremental backups. It includes the only known platform independent "rmt" server program that hides Linux incompatibilities. The "rmt" server from the star package implements all Sun/GNU/Schily/BSD enhancements and allows any "rmt" client from any OS to contact any OS as server.

## VI. SPONSOR INFORMATION

---

This Issue is Sponsored by: SecurityFocus

We are pleased to announce the launch of two new mailing lists for the Security community:

1. Security Management ([security-management-subscribe@securityfocus.com](mailto:security-management-subscribe@securityfocus.com))
2. Bugtraq-French ([bugtraq-french-subscribe@securityfocus.com](mailto:bugtraq-french-subscribe@securityfocus.com))

To subscribe to either of these lists, send mail to the listserv at the respective address indicated above; the subject and body of your message do not matter. Or, you can visit our signup page at <http://www.securityfocus.com/archive>

---

KaVaDo provides the first and only integrated Web application scanner and firewall security suite that prevent Web applications attacks, the most common form of online exploitation. Download a FREE whitepaper on Security Policy Automation for Web Applications.

<http://www.securityfocus.com/sponsor/KaVaDo> focus-ms 030818

---