

# SecurityFocus Microsoft Newsletter #167

**Source:** <http://www.derkeiler.com/Mailing-Lists/securityfocus/focus-ms/2003-12/0028.html>

---

**From:** Marc Fossi ([mfossi\\_at\\_securityfocus.com](mailto:mfossi_at_securityfocus.com))

**Date:** 12/16/03

Date: Mon, 15 Dec 2003 17:21:49 -0700 (MST)

To: Focus-MS <[focus-ms@securityfocus.com](mailto:focus-ms@securityfocus.com)>

SecurityFocus Microsoft Newsletter #167

---

This Issue is Sponsored by: SPIDynamics

Test for the Top Web Application Vulnerabilities- FREE Product Trial

Hackers are exploiting web apps with attacks such as; SQL Injection, XSS and Session Hijacking, all undetectable by Firewalls and IDS!  
Are you vulnerable? Run a FREE Test of your Web Apps via our FREE 15 Day Product Trial that delivers a comprehensive Vulnerability Report.

[http://www.securityfocus.com/sponsor/SPIDynamics\\_ms-secnews\\_031215](http://www.securityfocus.com/sponsor/SPIDynamics_ms-secnews_031215)

---

## I. FRONT AND CENTER

1. Worm Propagation In Protected Networks
2. RETRO-FOCUS
3. IP Spoofing: An Introduction

## II. MICROSOFT VULNERABILITY SUMMARY

1. EZMeeting EZNet.EXE Long HTTP Request Remote Buffer Overflow...
2. Abyss Web Server Authentication Bypass Vulnerability
3. MyServer HTTP File Name Request Handler Remote Denial Of Ser...
4. Multiple Browser URI Display Obfuscation Weakness
5. Multiple Vendor XML Parser SOAP Server Denial Of Service Vul...
6. Microsoft Roaming Profile Resource Quota Bypass Weakness
7. FlashGet Insecure Dialup Credential Storage Vulnerability
8. Multiple Vendor XML DTD Parameter Entity SOAP Server Denial ...

## III. MICROSOFT FOCUS LIST SUMMARY

1. Blessed Windows Security Templates (Thread)
2. How to disable all floppy drives on the network (Thread)
3. Article Announcement: Worm Propagation In Protected ... (Thread)
4. SecurityFocus Microsoft Newsletter #166 (Thread)

## IV. NEW PRODUCTS FOR MICROSOFT PLATFORMS

1. AccessMaster
2. KeyGhost SX
3. SafeKit

4. SecurDataStor
5. Proactive Windows Security Explorer
6. Outpost Personal Firewall Pro 2.0

#### V. NEW TOOLS FOR MICROSOFT PLATFORMS

1. Cryptonit v0.9.1
2. OpenSSL 0.9.7c
3. mrtg v2.10.7
4. Generic Security Service v0.0.7
5. Enigmail v0.82.3
6. Stealth HTTP Security Scanner v2.0b36

#### VI. UNSUBSCRIBE INSTRUCTIONS

#### VII. SPONSOR INFORMATION

#### I. FRONT AND CENTER

---

1. Worm Propagation In Protected Networks  
By SecurityFocus

Many documents explore worm propagation methods across the global Internet. In contrast, this analysis focuses on the impact of three prominent worms (Blaster, Slammer, and Code Red I/II) inside protected networks, once the security perimeter has been breached.

<http://www.securityfocus.com/infocus/1752>

2. Due to an increase in interest, SecurityFocus has decided to bring back past Infocus articles still relevant to the security industry. These articles will be posted at the bottom of the homepage, in the middle column.

3. IP Spoofing: An Introduction  
By Matthew Tanase  
Published March 11, 2003

IP spoofing allows an attacker to gain unauthorized access to a computer or a network by making it appear that a malicious message has come from a trusted machine by ?spoofing? the IP address of that machine. In this article, we will examine the concepts of IP spoofing: why it is possible, how it works, what it is used for and how to defend against it.

<http://www.securityfocus.com/infocus/1674>

#### II. MICROSOFT VULNERABILITY SUMMARY

---

1. EZMeeting EZNet.EXE Long HTTP Request Remote Buffer Overflow...  
BugTraq ID: 9167  
Remote: Yes  
Date Published: Dec 08 2003  
Relevant URL: <http://www.securityfocus.com/bid/9167>  
Summary:  
eZ is a commercially available conferencing software package distributed

and maintained by eZmeeting. It is available for the Microsoft Windows platform.

A vulnerability has been identified in the handling of some types of requests by the eZ package. Because of this, it may be possible for a remote attacker to execute arbitrary code and gain unauthorized access to a vulnerable host.

The problem is in the handling of long HTTP requests by the eZnet.exe component. When the software is executed, this component listens on port 80 of the system network interface for incoming conferencing connections.

When a request of excessive length is passed to a parameter of a valid component, the data is copied directly to the stack of the process. By requesting the component with a maliciously crafted string, it is possible to overwrite the stack with arbitrary data, forcing the process to execute attacker-supplied instructions with the privileges of the eZnet.exe process.

## 2. Abyss Web Server Authentication Bypass Vulnerability

BugTraq ID: 9171

Remote: Yes

Date Published: Dec 08 2003

Relevant URL: <http://www.securityfocus.com/bid/9171>

Summary:

Abyss Web Server is a freely available personal web server. It is maintained by Aprelium Technologies and runs on Microsoft Windows operating systems, as well as Linux.

A vulnerability has been reported to exist in the software that may allow a remote attacker to bypass authentication in order to access the resources. It has been reported that this issue only presents itself if the server is installed on a Linux system running FAT32. An attacker may access the password protected directory under which the server is running by adding a period as '.' or '%2e' at the end of a URL request. It has also been reported that adding a space ' ' or colon ':' to a URL may have the same affect, however it may also just cause a 404 server error.

Successful exploitation of this issue may allow an attacker to bypass authentication and gain access to server resources in order to launch further attacks.

Abyss Web Server versions prior to 1.2 have been reported prone to this issue.

## 3. MyServer HTTP File Name Request Handler Remote Denial Of Ser...

BugTraq ID: 9172

Remote: Yes

Date Published: Dec 08 2003

Relevant URL: <http://www.securityfocus.com/bid/9172>

Summary:

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

MyServer has been reported prone to a remotely triggered denial of service vulnerability. The issue presents itself when a remote attacker requests a file that contains spaces in its name. This activity will cause an exception in the affected server, effectively denying service to legitimate users.

An attacker may exploit this vulnerability to deny service to legitimate users.

#### 4. Multiple Browser URI Display Obfuscation Weakness

BugTraq ID: 9182

Remote: Yes

Date Published: Dec 09 2003

Relevant URL: <http://www.securityfocus.com/bid/9182>

Summary:

A weakness has been reported in multiple browsers that may allow attackers to obfuscate the URI for a visited page. The problem is said to occur when a URI designed to pass access a specific location with a supplied username, contains a non-printable hexadecimal value prior to the @ symbol.

Specifically, the malicious URI must be formatted as follows, where %00 may be any non-displayable hexadecimal value:

<http://www.trusted.com%00@www.malicious.com>

Upon clicking the link, the URI field would contain www.trusted.com despite the access site actually being www.malicious.com. It should be noted that manually placing such a URI into the location may not work, as the hexadecimal value must not be escaped.

An attacker could exploit this issue by supplying a malicious URI pointing to a page designed to mimic that of a trusted site. If an unsuspecting victim were to follow the link and attempt to verify the authenticity of the current location by checking the current URI, they may be deceived into believing they are at the actual trusted site. This could potentially cause a false sense of security for the victim.

There are currently conflicting reports regarding which versions of Internet Explorer this weakness affects, including versions for Mac OS X. As more information becomes available the necessary clarifications will be addressed.

Symantec has confirmed however, that this issue does affect the latest Internet Explorer with all service packs and patches applied.

Reports indicate that Microsoft Outlook Express 6 is affected by this issue as well. As such, it is believed that all releases of Outlook Express and possibly Outlook are affected.

Mozilla and Mozilla Firebird browsers are also vulnerable to this issue. This has not yet been confirmed.

#### 5. Multiple Vendor XML Parser SOAP Server Denial Of Service Vul...

BugTraq ID: 9185

Remote: Yes

Date Published: Dec 09 2003

Relevant URL: <http://www.securityfocus.com/bid/9185>

Summary:

SOAP is the Simple Object Access Protocol, which is implemented in numerous web service software packages by various vendors. SOAP servers are available for the Unix, Linux, and Microsoft Windows platforms.

A problem has been identified in several different SOAP servers when handling certain types of requests. Because of this, it is possible for an attacker to force a denial of service on systems using a vulnerable implementation.

The problem is in the handling of specially crafted SOAP requests. By making a SOAP request with maliciously crafted XML data, it is possible to cause the SOAP server to consume excessive amounts of system resources. This issue can be used to make the server unavailable while it handles the requests, and could be continuously used to create a prolonged denial of web services.

#### 6. Microsoft Roaming Profile Resource Quota Bypass Weakness

BugTraq ID: 9186

Remote: No

Date Published: Dec 09 2003

Relevant URL: <http://www.securityfocus.com/bid/9186>

Summary:

Microsoft proquota.exe is an application used to enforce limits on profile storage space available on a server for each roaming profile.

Proquota has been reported prone to a weakness that may be exploited by a local user to bypass profile storage limits supposedly enforced by the proquota application. It has been reported that an attacker who has interactive access to a system, may make the proquota application behave in an unstable manner by having an open unsaved notepad session active when a "Log Off" procedure is invoked from the start menu.

It has been reported that when the "End Now" dialog appears for the unclosed notepad session, the attacker may cause the proquota.exe application process to crash, by hovering the mouse pointer over the proquota icon in the system systray.

Once the proquota application has failed, it has been reported that the attacker may proceed without any resource limits being enforced on the size of the current profile. An attacker may exploit this condition to consume resources on the associated domain controller server, ultimately causing the domain controller to behave in an unstable manner.

#### 7. FlashGet Insecure Dialup Credential Storage Vulnerability

BugTraq ID: 9192

Remote: No

Date Published: Dec 10 2003

Relevant URL: <http://www.securityfocus.com/bid/9192>

Summary:

FlashGet is a download manager for Microsoft Windows platforms.

FlashGet allows users to store credentials for dialup connections. This feature is prone to a vulnerability. In particular, FlashGet stores dialup credentials in a user-accessible registry key. These credentials are stored in the following registry key:

[HKEY\_USERS\DEFAULT\Software\JetCar\JetCar\DialUp

The username will be stored in plaintext and the password will be hex-encoded. As a result, malicious local users may obtain these credentials. This presents a security risk if dialup accounts are not shared between users on the system.

This issue was reported in FlashGet 0.9 through 1.2. Other versions may also be affected.

#### 8. Multiple Vendor XML DTD Parameter Entity SOAP Server Denial ...

BugTraq ID: 9204

Remote: Yes

Date Published: Dec 11 2003

Relevant URL: <http://www.securityfocus.com/bid/9204>

Summary:

SOAP is the Simple Object Access Protocol, which is implemented in numerous web service software packages by various vendors. SOAP servers are available for the Unix, Linux, and Microsoft Windows platforms.

XML DTD (Document Type Definition) defines how XML markup tags should be interpreted by the application handling the XML document.

A problem has been identified in several different SOAP servers when handling certain types of SOAP requests. Because of this, it is possible for an attacker to force a denial of service on systems using a vulnerable implementation.

The problem is in the handling of SOAP requests that contain references to DTD parameter entities. By making a SOAP request with maliciously crafted DTD data, it is possible to cause the SOAP server to consume excessive amounts of system resources. This issue can be used to make the server unavailable while it handles the requests, and could be continuously used to create a prolonged denial of web services.

### III. MICROSOFT FOCUS LIST SUMMARY

---

#### 1. Blessed Windows Security Templates (Thread)

Relevant URL:

<http://www.securityfocus.com/archive/88/347385>

2. How to disable all floppy drives on the network (Thread)

Relevant URL:

<http://www.securityfocus.com/archive/88/347265>

3. Article Announcement: Worm Propagation In Protected ... (Thread)

Relevant URL:

<http://www.securityfocus.com/archive/88/347120>

4. SecurityFocus Microsoft Newsletter #166 (Thread)

Relevant URL:

<http://www.securityfocus.com/archive/88/346925>

#### IV. NEW PRODUCTS FOR MICROSOFT PLATFORMS

##### 1. AccessMaster

By: Evidian Inc.

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

Relevant URL: <http://www.evidian.com/accessmaster/about/index.htm>

Summary:

Extending onto a networked world means embracing the unknown. Piracy, vandalism, industrial espionage... – attacks on companies are doubling each year. With uniquely integrated security software, AccessMaster manages and safeguards access to your data, end-to-end, from portals to legacy, and lets you enforce a single, unified security policy across the enterprise and beyond.

AccessMaster ensures high security level by federating your existing security solutions, while ensuring at the same time user's convenience with Single Sign-On and security officer's ease of administration with centralized, Ldap-compliant, user and PKI management. In this way, AccessMaster reduces IT security cost of ownership, with rapid return on investment.

AccessMaster is recognized by analysts as a leading security suite for large enterprises today. It was awarded "best access control" software by Secure Computing Magazine three years running, in 2000, 2001, and 2002.

##### 2. KeyGhost SX

By: KeyGhost Ltd

Platforms: BeOS, DOS, Linux, OS/2, Solaris, SunOS, Windows 2000, Windows 95/98, Windows NT, Windows XP

Relevant URL: <http://www.keyghost.com/SX/>

Summary:

KeyGhost SX discreetly captures and records all keystrokes typed, including chat conversations, email, word processor, or even activity within an accounting or specialist system. It is completely undetectable by software scanners and provides you with one of the most powerful stealth surveillance applications offered anywhere.

Because KeyGhost uses STRONG 128-Bit encryption to store the recorded data in its own internal memory (not on the hard drive), it is impossible for a network intruder to gain access to any sensitive data stored within the device.

### 3. SafeKit

By: Evidian Inc.

Platforms: AIX, HP-UX, Linux, Solaris, Windows 2000

Relevant URL: <http://www.evidian.com/safekit/index.htm>

Summary:

Evidian's SafeKit technology makes it possible to render any application available 24 hours per day. With no extra hardware: just use your existing servers and install this software-only solution.

This provides ultimate scalability. As your needs grow, all you need to do is add more standard servers into the cluster. With the load balancing features of SafeKit, you can distribute applications over multiple servers. If one system fails completely, the others will continue to serve your users.

### 4. SecurDataStor

By: encryptX Corporation

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

Relevant URL: <http://www.encryptx.com/products/securdatastor.asp>

Summary:

The SecurDataStor product line is designed to provide a comprehensive software security solution that manages and controls access to sensitive information that you need to share internally and externally. SecurDataStor is available in three versions: Basic, Premium, and Platinum. Depending on the level of security that you need, you can choose the SecurDataStor product that suits your needs.

With its end-to-end protection of sensitive business information, SecurDataStor products protect sensitive information when used by the originator, stored locally on a hard drive or file server, and when shared. Users can safely share sensitive information across different Microsoft Windows operating systems, over different network and firewall technologies, and across different forms of removable media.

### 5. Proactive Windows Security Explorer

By: Elcomsoft Co. Ltd.

Platforms: Windows 2000, Windows NT, Windows XP

Relevant URL: <http://www.elcomsoft.com/pwsex.html#>

Summary:

Proactive Windows Security Explorer (PWSEX) is a password security test tool that's designed to allow Windows NT, Windows 2000, and Windows XP-based systems administrators to identify and close security holes in their networks. Proactive Windows Security Explorer helps secure networks by executing an audit of account passwords, and exposing insecure account passwords. If it is possible to recover the password within a reasonable time, the password is considered insecure.

An administrator can also use it to recover any lost password and access a user's Windows account. Proactive Windows Security Explorer works by analyzing user password hashes and recovering plain-text passwords.

6. Outpost Personal Firewall Pro 2.0

By: Agnitum

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

Relevant URL: <http://www.outpost.uk.com>

Summary:

New Outpost Personal Firewall Pro 2.0 outdistances the award-winning Outpost Personal Firewall Pro 1.0 on multiple levels, from enhanced privacy features to ease-of-use. As the foremost security application for personal computers, Outpost Personal Firewall Pro 2.0 gives you the latest in personal firewall technology, making version 2.0 the clear security choice for your system.

## V. NEW TOOLS FOR MICROSOFT PLATFORMS

---

1. Cryptonit v0.9.1

By: IDEALX <idx-pki@idealx.org>

Relevant URL: <http://cryptonit.org/>

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

Summary:

Cryptonit is a client side cryptographic tool which allows you to encrypt/decrypt and sign/verify files with PKI (Public Key Infrastructure) certificates.

2. OpenSSL 0.9.7c

By: The OpenSSL Project Team <openssl@openssl.org>

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

Platforms: UNIX, Windows NT

Summary:

The OpenSSL Project is a collaborative effort to develop a robust, commercial-grade, fully featured, and Open Source toolkit implementing the Secure Sockets Layer (SSL v2/v3) and Transport Layer Security (TLS v1) as well as a full-strength general-purpose cryptography library.

3. mrtg v2.10.7

By: Tobias Oetiker

Relevant URL: <http://people.ee.ethz.ch/~oetiker/webtools/mrtg/>

Platforms: POSIX, Windows 2000, Windows NT

Summary:

The Multi Router Traffic Grapher (MRTG) is a tool to monitor the traffic load on network-links. MRTG generates HTML pages containing GIF/PNG images which provide a live visual representation of this traffic.

4. Generic Security Service v0.0.7

By: Simon Josefsson

Relevant URL: <http://www.gnu.org/software/gss/>

Platforms: UNIX, Windows 2000, Windows NT, Windows XP

Summary:

A bug that prevented 3DES gss\_wrap from working in the Kerberos 5 mechanism was fixed. The library headers file now works even when the Kerberos 5 mechanism is disabled. The package has been tested on more platforms.

5. Enigmail v0.82.3

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.

6. Stealth HTTP Security Scanner v2.0b36

By: Felipe Moniz, Security Specialist

Relevant URL: <http://www.hideaway.net/stealth>

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

Summary:

Stealth 1.0 scans for 2883 HTTP vulnerabilities. This tool is designed especially for the system administrators, security consultants and IT professionals to check the possible security holes and to confirm any present security vulnerabilities that hackers can exploit. Totally free for commercial and non-commercial use.

VI. UNSUBSCRIBE INSTRUCTIONS

---

To unsubscribe send an e-mail message to [ms-secnews-unsubscribe@securityfocus.com](mailto: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](mailto:listadmin@securityfocus.com) and ask to be manually removed.

VII. SPONSOR INFORMATION

---

This Issue is Sponsored by: SPIDynamics

Test for the Top Web Application Vulnerabilities– FREE Product Trial

Hackers are exploiting web apps with attacks such as; SQL Injection, XSS and Session Hijacking, all undetectable by Firewalls and IDS! Are you vulnerable? Run a FREE Test of your Web Apps via our FREE 15 Day Product Trial that delivers a comprehensive Vulnerability Report.

[http://www.securityfocus.com/sponsor/SPIDynamics\\_ms-secnews\\_031215](http://www.securityfocus.com/sponsor/SPIDynamics_ms-secnews_031215)

---

---

---