

# SecurityFocus Microsoft Newsletter #147

**Source:** <http://www.derkeiler.com/Mailing-Lists/securityfocus/focus-ms/2003-07/0099.html>

---

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

**Date:** 07/28/03

Date: Mon, 28 Jul 2003 14:53:46 -0600 (MDT)

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

SecurityFocus Microsoft Newsletter #147

---

This Issue is Sponsored by: SPI Dynamics

## ALERT:

"How a Hacker Launches a LDAP Injection Attack Step-by-Step" – White Paper  
It's as simple as placing additional LDAP query commands into a Web form input box giving hackers complete access to all your backend systems!  
Firewalls and IDS will not stop such attacks because LDAP Injections are seen as valid data.

Download this \*FREE\* white paper from SPI Dynamics for a complete guide to protection!

<http://www.securityfocus.com/SPIDynamics-ms-secnews6>

---

## I. FRONT AND CENTER

1. "Copying is Theft ..."
2. Demonstrating ROI for Penetration Testing (Part One)

## II. MICROSOFT VULNERABILITY SUMMARY

1. SimpNews PATH\_SIMPNEWS Remote File Include Vulnerability
2. Drupal Cross-Site Scripting Vulnerability
3. SurfControl E-Mail Filter For SMTP Nested Zip File Filter...
4. MoreGroupWare WEBMAIL2\_INC\_DIR Remote File Include Vulnerability
5. Microsoft MSN Messenger Image File Transfer Denial of Service...
6. RAV AntiVirus Online Virus Scan RavonLine.DLL ActiveX Control...
7. Microsoft Windows 2000 RPC DCOM Interface Denial of Service...
8. Microsoft Multiple IIS 6.0 Web Admin Vulnerabilities

## III. MICROSOFT FOCUS LIST SUMMARY

1. Tracking down a user in a large AD network (Thread)
2. SecurityFocus Microsoft Newsletter #146 (Thread)
3. plugging old IIS FTP holes (Thread)
4. Article Announcement: Waiting for the Worms (Thread)
5. Article Announcement: Forensic Log Parsing with Microsoft's...
6. Biometric fingerprint scanner (Thread)

## IV. NEW PRODUCTS FOR MICROSOFT PLATFORMS

1. Aluria's Spyware Eliminator
2. ipANGEL
3. AES PRO

#### V. NEW TOOLS FOR MICROSOFT PLATFORMS

1. Enigmail v0.81.0
2. RatScan v1.2
3. DisSpam v0.11

#### VI. SPONSOR INFORMATION

##### I. FRONT AND CENTER

---

1. "Copying is Theft ..."

By Mark Rasch

And other legal myths in the looming battle over peer-to-peer.

<http://www.securityfocus.com/columnists/175>

2. Demonstrating ROI for Penetration Testing (Part One)

By Marcia Wilson

This is the first in a series of articles demonstrating ROI (return on investment) for a penetration test. You will have to step into the world of budgeting, cost justification, resource allocation, and learn a few unfamiliar terms.

<http://www.securityfocus.com/infocus/1715>

##### II. BUGTRAQ SUMMARY

---

1. SimpNews PATH\_SIMPNEWS Remote File Include Vulnerability

BugTraq ID: 8227

Remote: Yes

Date Published: Jul 18 2003 12:00AM

Relevant URL:

<http://www.securityfocus.com/bid/8227>

Summary:

SimpNews is a web news system implemented in PHP. It is available for Unix/Linux variants and Microsoft Windows operating systems.

SimpNews is prone to a vulnerability that may permit remote attackers to include and execute malicious PHP scripts. Remote users, under some PHP configurations, may influence the \$path\_simpnews URI variable. This variable is used in the include path for the 'config.php', 'functions.php' and 'includes/has\_entries.inc' scripts. By influencing the include path so that it points to a malicious PHP script on a remote system, it is possible to cause arbitrary PHP code to be executed. This would occur in the context of the web server. This issue exists in both the 'eventcal2.php' and 'eventscroller.php' scripts.

This could be exploited to execute malicious PHP commands in the context of the web server process.

It should be noted that although SimpNews versions 2.01 through 2.13 have been reported vulnerable, other versions might also be affected.

## 2. Drupal Cross-Site Scripting Vulnerability

BugTraq ID: 8235

Remote: Yes

Date Published: Jul 21 2003 12:00AM

Relevant URL:

<http://www.securityfocus.com/bid/8235>

Summary:

Drupal is an open-source content management system. Drupal is available for a number of platforms including Microsoft Windows operating systems and Unix/Linux variants.

The Drupal content management system is prone to a cross-site scripting vulnerability. This issue is exposed through the main page and through other sub-pages. An attacker may exploit this issue by including hostile HTML and script code in a malicious link to Drupal. This code may be rendered in the web browser of a user who visits the link. This would occur in the security context of the site hosting Drupal.

The attacker-supplied HTML and script code would be able to access properties of the site, potentially allowing for theft of cookie-based authentication credentials. An attacker could also exploit this issue to control how the site is rendered to the user.

## 3. SurfControl E-Mail Filter For SMTP Nested Zip File Filter Bypass Vulnerability

BugTraq ID: 8240

Remote: Yes

Date Published: Jul 20 2003 12:00AM

Relevant URL:

<http://www.securityfocus.com/bid/8240>

Summary:

SurfControl E-Mail Filter for SMTP is a gateway e-mail scanner that is compatible with a number of SMTP server implementations. It is available for Microsoft Windows operating systems.

It is reported that nested zip files may bypass the scanning mechanism in Surf Control E-Mail Filter for SMTP. If a zipped message attachment contains 16 other zip files, the filter will scan the first 15 files but fail to scan the 16th. Scanning is reportedly done alphabetically so it is possible to control the order in which files are scanned.

This could permit content that is malicious or restricted by security policy to bypass the e-mail filter. An end-user would still be required

to execute any malicious content that is sent via this medium.

This issue may be exploitable with other archive formats. Other SurfControl products may also use a similar scanning mechanism and may be prone to this issue as well, though this has not been confirmed.

#### 4. MoreGroupWare WEBMAIL2\_INC\_DIR Remote File Include Vulnerability

BugTraq ID: 8249

Remote: Yes

Date Published: Jul 23 2003 12:00AM

Relevant URL:

<http://www.securityfocus.com/bid/8249>

Summary:

moregroupware is a tool to facilitate office communications. It includes, among other features, webmail, calendaring and project management functionality. It is implemented in PHP and is available for a variety of platforms including Microsoft Windows and Linux and Unix variant operating environments.

moregroupware is prone to a vulnerability that may permit remote attackers to include and execute malicious PHP scripts. Remote users, under some PHP configurations, may influence the \$webmail2\_inc\_dir URI variable or in some cases the \$appconf URI variable. This variable is used in the include path for the 'mimepart.php', 'pear.php' and 'mime\_types.php' scripts. By influencing the include path so that it points to a malicious PHP script on a remote system, it is possible to cause arbitrary PHP code to be executed. This would occur in the context of the web server. This issue exists in 'class.html.mime.mail.inc', 'rfc822.php' and 'webmail2\_func.inc' scripts.

This could be exploited to execute malicious PHP commands in the context of the web server process.

It should be noted that although moregroupware version 0.6.8 has been reported vulnerable, other versions might also be affected.

#### 5. Microsoft MSN Messenger Image File Transfer Denial of Service Vulnerability

BugTraq ID: 8221

Remote: Yes

Date Published: Jul 17 2003 12:00AM

Relevant URL:

<http://www.securityfocus.com/bid/8221>

Summary:

MSN Messenger is an instant messaging client for Microsoft Windows systems, based on the Passport system.

MSN Messenger is reportedly prone to a denial of service.

It has been alleged that when certain malformed image files are received via a Messenger file transfer, Messenger may fail. Reportedly, many malformed images would have to be received in succession in order to exploit this vulnerability.

The exact cause of this vulnerability is not currently known. This record will be updated when further information becomes available.

#### 6. RAV AntiVirus Online Virus Scan RavonLine.DLL ActiveX Control Buffer Overflow Vulnerability

BugTraq ID: 8225

Remote: Yes

Date Published: Jul 18 2003 12:00AM

Relevant URL:

<http://www.securityfocus.com/bid/8225>

Summary:

ravonline.dll is a linked library distributed as part of the ActiveX control for the RAV AntiVirus Online Virus Scan service.

ravonline.dll has been reported prone to a buffer overflow vulnerability. The issue reportedly presents itself when excessive data is passed to the browseForFolder() function.

It has been conjectured that this issue could potentially lead to the execution of code with the privileges of the user executing the web browser. This problem requires that a user with the vulnerable control installed visit a web page that invokes the control in a manner sufficient to trigger the issue. Upon doing so, it may be possible to create a remotely exploitable stack overflow condition that results in the overwriting of sensitive process memory. This, however, has not been confirmed.

Although unconfirmed, because the function browseForFolder() is reportedly imported from Shell32.dll, this issue may actually present itself in Microsoft Windows native Shell32.dll library.

It should be noted, that ActiveX controls by nature might contain latent vulnerabilities. Caution should be employed if installing ActiveX controls.

#### 7. Microsoft Windows 2000 RPC DCOM Interface Denial of Service Vulnerability

BugTraq ID: 8234

Remote: Yes

Date Published: Jul 21 2003 12:00AM

Relevant URL:

<http://www.securityfocus.com/bid/8234>

Summary:

Microsoft Windows uses Remote Procedure Calls (RPC) for client-server communications in a distributed computing environment (DCE). TCP Port 135 is typically used for DCE endpoint resolution.

A vulnerability in the Windows DCE-RPC stack could allow a remote user to disable RPC services. If a specifically malformed packet is sent to the DCOM \_\_RemoteGetClassObject interface on a vulnerable system, the RPC service may fail. This is due to a NULL pointer being passed from \_\_RemoteGetClassObject to the PerformScmStage function.

Because other services may depend on the RPC service, the loss of this interface may impact other components on the system, possibly causing them to fail as well.

It should be noted that once disabled, it might be possible for local users to gain elevated privileges by hijacking orphaned pipes left by the RPC process. This issue is described in BID 6769.

This issue may be related to BID 6005, however, this has not been confirmed. Reportedly, this vulnerability affects systems that have applied the patch for Microsoft Security Bulletin MS03-026.

#### 8. Microsoft Multiple IIS 6.0 Web Admin Vulnerabilities

BugTraq ID: 8244

Remote: Yes

Date Published: Jul 22 2003 12:00AM

Relevant URL:

<http://www.securityfocus.com/bid/8244>

Summary:

Multiple vulnerabilities have been reported in the web admin interface that is included in Microsoft IIS 6.0.

Multiple instances of cross-site scripting vulnerabilities were discovered in many of the ASPs that are included in the web admin interface. In particular, input supplied to the ReturnURL parameter via many of these scripts (such as Web\_LogSettings.asp) may not be sanitized before being echoed back to a user of the interface. An attacker could exploit these issues via a malicious link to the interface that contains hostile HTML or script code. This could cause attacker-supplied code to be rendered in the web browser of a legitimate interface user who follows the link.

Additionally, it is reported that the web admin interface could expose valid session IDs or permit unauthorized access to areas that do not require session IDs. These issues may in part be due to insufficient access validation for certain web admin interface components. Scripts that may be affected include default.asp, tasks.asp and users.asp.

This BID will be separated into separate BIDs when further analysis of these issues is complete.

### III. MICROSOFT FOCUS LIST SUMMARY

---

1. Tracking down a user in a large AD network (Thread)

Relevant URL:

<http://www.securityfocus.com/archive/88/330458>

2. SecurityFocus Microsoft Newsletter #146 (Thread)

Relevant URL:

<http://www.securityfocus.com/archive/88/329805>

3. plugging old IIS FTP holes (Thread)

Relevant URL:

<http://www.securityfocus.com/archive/88/329771>

4. Article Announcement: Waiting for the Worms (Thread)

Relevant URL:

<http://www.securityfocus.com/archive/88/329732>

5. Article Announcement: Forensic Log Parsing with Microsoft's LogParser (Thread)

Relevant URL:

<http://www.securityfocus.com/archive/88/329729>

6. Biometric fingerprint scanner (Thread)

Relevant URL:

<http://www.securityfocus.com/archive/88/329727>

### IV. NEW PRODUCTS FOR MICROSOFT PLATFORMS

---

1. Aluria's Spyware Eliminator

by Aluria Software

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

Relevant URL:

<http://www.aluriasoftware.com/spywareeliminator/index.html>

Summary:

Aluria's Spyware Eliminator protects you from the Spyware epidemic. While anti-virus software guards you from viruses, it does not prevent Spyware from attacking your computer. Aluria's Spyware Eliminator not only detects and removes Spyware, Adware and Keyloggers from your computer, but now actively blocks Spyware and Adware when your computer is under assault.

2. ipANGEL

by Lucid Security

Platforms: Os Independent

Relevant URL:

<http://www.lucidsecurity.com/products.php>

Summary:

Lucid Security's ipANGEL, coupled with Check Point FireWall-1, provides complete protection against all network and application attacks. ipANGEL marks a departure from the traditional thinking of what an intrusion prevention product should do. It detects and shields vulnerable applications without duplicating the capabilities of the firewall. Lucid Security purposefully limited ipANGEL's scope:

- Operates exclusively with FireWall-1
- Does not duplicate FireWall-1's capabilities
- Ignores traffic that is not an attack against vulnerable applications and systems

This approach has enabled Lucid Security to focus on building the intelligence and automation that make ipANGEL easy to deploy and maintain. Together, ipANGEL and FireWall-1 actively defend against attacks in real time.

### 3. AES PRO

by Workable Resources

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

Relevant URL:

<http://www.aes.safeworld.info/pro.htm>

Summary:

AES Pro is the utility program that creates active public keys. Active key is an executable program that contains a public key and the software necessary to encrypt messages and decrypt the answer-back messages. Users can create active public keys that anyone can use to encrypt messages. No other software is required. These active public keys are ideal to create communication with the users who do not have the PGP or CHAOS Public Key programs installed.

## V. NEW TOOLS FOR MICROSOFT PLATFORMS

---

### 1. Enigmail v0.81.0

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.

## 2. RatScan v1.2

by BeetleSoft

Relevant URL:

<http://www.beetlesoft.com/products.html>

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

Summary:

'RatScan' a security tool and front-end for the RATS scanner which can check your source code for weaknesses, vulnerabilities and exploits. It can detect potentially dangerous coding practices and advise you on the risks and the various steps needed to secure your code further. It is compatible with multiple programming languages including PHP, C/C++, Perl and others.

## 3. DisSpam v0.11

by Mina Naguib

Relevant URL:

<http://online.securityfocus.com/tools/2563>

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

Summary:

DisSpam is a personal solution to combat spam (i.e. not for mailservers/ISPs). It is a Perl script that removes spam from POP3 mailboxes based on RBLs such as orbz.org. It runs through cron and uses a very simple configuration file.

## VI. SPONSOR INFORMATION

-----  
This Issue is Sponsored by: SPI Dynamics

ALERT:

"How a Hacker Launches a LDAP Injection Attack Step-by-Step" – White Paper  
It's as simple as placing additional LDAP query commands into a Web form input box giving hackers complete access to all your backend systems!  
Firewalls and IDS will not stop such attacks because LDAP Injections are seen as valid data.

Download this \*FREE\* white paper from SPI Dynamics for a complete guide to protection!

<http://www.securityfocus.com/SPIDynamics-ms-secnews6>  
-----

-----  
Your network firewall and IDS products do not prevent Web application attacks – the most common form of online exploitation– resulting in Web defacement, data theft, sabotage and fraud.

KaVaDo is the only company that provides a complete suite of Web application security products.

Download a FREE whitepaper on "Security Policy Automation for Web Applications": <http://www.securityfocus.com/Kavado-focus-ms>

---