

SecurityFocus Microsoft Newsletter #120

Source: <http://www.derkeiler.com/Mailing-Lists/securityfocus/focus-ms/2003-01/0002.html>

From: Marc Fossi (mfossi@securityfocus.com)

Date: 01/06/03

Date: Mon, 6 Jan 2003 11:50:05 -0700 (MST)

From: Marc Fossi <mfossi@securityfocus.com>

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

SecurityFocus Microsoft Newsletter #120

This issue is sponsored by: Qualys

Strengthening Network Security: FREE Guide Network security is a constantly moving target – even proven solutions lose their punch over time. Find out how to get COMPLETE PROTECTION against ever-growing security threats with our FREE new Guide.

Get your copy today at: https://www.qualys.com/forms/nsguideh_376.php

I. FRONT AND CENTER

1. Exchange 2000 in the Enterprise: Tips and Tricks Part One
2. Windows Forensics: A Case Study, Part 1
3. The Briscoe Syndrome
4. SecurityFocus DPP Program
5. InfoSec World Conference and Expo/2003 (March 10–12, 2003, Orlando, FL)

II. MICROSOFT VULNERABILITY SUMMARY

1. Microsoft Windows File Protection Code–Signing Verification...
2. Microsoft Windows File Protection Signed File Replacement...
3. Microsoft Internet Explorer Multimedia Page Cross–Site...
4. PlatinumFTPserver Information Disclosure Vulnerability
5. PlatinumFTPserver Arbitrary File Deletion Vulnerability
6. PlatinumFTPserver Denial Of Service Vulnerability
8. PHP wordwrap() Heap Corruption Vulnerability
9. Gallery Remote Code Execution Vulnerability

III. MICROSOFT FOCUS LIST SUMMARY

1. Account Management (Thread)
2. SecurityFocus Microsoft Newsletter #119 (Thread)
3. MDAC 2.7 SP1 now available as a standalone install (Thread)

IV. NEW PRODUCTS FOR MICROSOFT PLATFORMS

1. East–Tec FormatSecure
2. KillDisk
3. Norton SystemWorks 2003

V. NEW TOOLS FOR MICROSOFT PLATFORMS

1. DumpWin v2.0
2. AnalogX Script Defender 1.01
3. pcInternet Patrol

VI. SPONSOR INFORMATION

I. FRONT AND CENTER

1. Exchange 2000 in the Enterprise: Tips and Tricks Part One

By Tim Mullen

In this two-part article we will discuss an alternate configuration in which we will utilize Microsoft's Internet Security and Acceleration (ISA) Server, a third party SMTP Gateway (Trend Micro's Internet Messaging Security Suite) and Exchange 2000. This sort of configuration is flexible enough to be used in smaller installations that do not use a DMZ, or as part of the DMZ configuration itself.

<http://online.securityfocus.com/infocus/1654>

2. Windows Forensics: A Case Study, Part One

by Stephen Barish

It's a security person's worst nightmare. You've just inherited a large, diverse enterprise with relatively few security controls when something happens. We all try to detect malicious activity at the perimeter of the network by monitoring our intrusion detection systems, and watching attackers bang futilely on our firewall. Even those attackers tricky enough to slip through the firewall bounce harmlessly off our highly secured servers, and trip alarms off throughout the network as they attempt to compromise it. Reality is usually somewhat different: most of us simply don't have the tools, or at least we don't have expensive, dedicated tools. But we do have ways to stop the pain.

<http://online.securityfocus.com/infocus/1653>

3. The Briscoe Syndrome

By Mark Rasch

Fear of terrorism and a desire to cooperate with law enforcement has led many corporate insiders to pony up sensitive information on their customers to anyone with a badge... with no court order required.

<http://online.securityfocus.com/columnists/132>

4. SecurityFocus DPP Program

Attention Universities!! Sign-up now for preferred pricing on the only global early-warning system for cyber attacks – SecurityFocus DeepSight Threat Management System.

Click here for more information:

<http://www.securityfocus.com/corporate/products/dpsection.shtml>

5. InfoSec World Conference and Expo/2003 (March 10–12, 2003, Orlando, FL)

Optional Workshops March 8, 9, 12, 13, & 14 Vendor Expo March 10 & 11

Solutions to today's security concerns; hands-on experts; blockbuster vendor expo; the CISO Executive Summit; invaluable networking opportunities. InfoSec World has it all!

Go to: <http://www.misti.com/10/os03nl37inf.html>

II. BUGTRAQ SUMMARY

1. Microsoft Windows File Protection Code–Signing Verification Weakness

BugTraq ID: 6482

Remote: Yes

Date Published: Dec 26 2002 12:00AM

Relevant URL:

<http://www.securityfocus.com/bid/6482>

Summary:

Microsoft Windows ships with a component to verify digital signatures that have been applied to system files and third-party code called 'Windows File Protection' (WFP). It has been reported that files signed using code–signing certificates issued by any trusted root CAs will be trusted by WFP. This includes operating system files and device drivers. Consequently, any attacker in possession of a code signing certificate rooted at any trusted CA may create malicious code signed with the certificate that will be trusted.

There are several root CAs preconfigured in Microsoft Windows. Some of these CAs may have dubious security practices. For example, some may issue SSL certificates without valid Key Usage, Enhanced Key Usage Object Identifier and Basic Constraints fields. This could result in the ability to use a SSL certificate to sign code which would be trusted by WFP. Furthermore, 'www.freessl.com' allegedly may be used by attackers to obtain certificates anonymously that are rooted at the trusted CA "usertrust.com".

While these faults may lie with the individual authorities, trusting root CAs for all signed code is a weakness in the design of Windows File Protection.

2. Microsoft Windows File Protection Signed File Replacement Vulnerability

BugTraq ID: 6483

Remote: No

Date Published: Dec 27 2002 12:00AM

Relevant URL:

<http://www.securityfocus.com/bid/6483>

Summary:

Microsoft Windows ships with a component to verify digital signatures that have been applied to system files and third-party code called 'Windows File Protection' (WFP). A vulnerability in Windows File Protection has been reported that may result in the re-introduction of vulnerable files after fixes/patches have replaced them.

According to the report, Security Catalogs containing the hashes of old files are kept in %WinDir%\System32\CatRoot after patches/fixes which replace them have been deployed. If these patched files are somehow overwritten with the vulnerable old files, Windows File Protection will not detect the old files as being invalid due to the existent catalog containing their hash.

This may allow for attackers to re-introduce onto a system and then exploit vulnerable executables/files.

3. Microsoft Internet Explorer Multimedia Page Cross-Site Scripting Vulnerability

BugTraq ID: 6481

Remote: Yes

Date Published: Dec 26 2002 12:00AM

Relevant URL:

<http://www.securityfocus.com/bid/6481>

Summary:

Microsoft Internet Explorer is prone to cross-site scripting attacks.

When a multimedia file is loaded by MSIE (such as a Macromedia SWF file), instead of loading the file directly, a separate page is generated which contains the URI of the file. HTML tags and script code are not filtered when the URI is displayed in this separate page. As a result, an attacker may create a malicious link which contains arbitrary script code. If a user of the vulnerable web browser visits such a link, the attacker-supplied script code will be interpreted by their browser. This will occur in the context of the website the link points to. An attacker may obfuscate this malicious link so that it seems innocuous.

An attacker may exploit this issue to steal cookie-based authentication credentials from web users. Other attacks are also possible.

4. PlatinumFTPServer Information Disclosure Vulnerability

BugTraq ID: 6492

Remote: Yes

Date Published: Dec 30 2002 12:00AM

Relevant URL:

<http://www.securityfocus.com/bid/6492>

Summary:

PlatinumFTPserver is a FTP server available for Microsoft Windows operating systems.

It has been reported that PlatinumFTPServer fails to properly sanitize some FTP commands. An attacker is able to traverse outside of the established FTP root by using dot-dot-slash (../) directory traversal sequences in conjunction with some FTP commands. Specifically, the attacker can use the DIR FTP command to obtain information about potentially sensitive files located on a vulnerable system outside of the FTP root directory.

Disclosure of sensitive system information may aid the attacker in launching further attacks against the target system.

This vulnerability was reported for PlatinumFTPserver 1.0.6. It is not known whether other versions are affected.

5. PlatinumFTPServer Arbitrary File Deletion Vulnerability

BugTraq ID: 6493

Remote: Yes

Date Published: Dec 30 2002 12:00AM

Relevant URL:

<http://www.securityfocus.com/bid/6493>

Summary:

PlatinumFTPserver is a FTP server available for Microsoft Windows operating systems.

It has been reported that PlatinumFTPServer fails to properly sanitize some FTP commands. An attacker is able to traverse outside of the established FTP root by using dot-dot-slash (../) directory traversal sequences in conjunction with some FTP commands. Specifically, the attacker can use the DELETE FTP command to delete arbitrary files outside of the FTP root directory. This may be exploited by the attacker to render a system completely unusable.

This vulnerability was reported for PlatinumFTPserver 1.0.6. It is not known whether other versions are affected.

6. PlatinumFTPserver Denial Of Service Vulnerability

BugTraq ID: 6494

Remote: Yes

Date Published: Dec 30 2002 12:00AM

Relevant URL:

<http://www.securityfocus.com/bid/6494>

Summary:

PlatinumFTPserver is a FTP server available for Microsoft Windows operating systems.

It has been reported that PlatinumFTPserver fails to properly sanitize FTP commands. By sending a malicious request to the vulnerable server, using directory traversal sequences, it is possible for a remote attacker to cause a denial of service condition.

An attacker can exploit this vulnerability by using specially crafted dot-dot-slash (../) directory traversal sequences in conjunction with the CD FTP command to cause a denial of service.

Restarting the vulnerable service will be necessary to restore functionality.

This vulnerability was reported for PlatinumFTPserver 1.0.6. It is not known whether other versions are affected.

7. Microsoft Visual SourceSafe Client-Side Access Control Weakness

BugTraq ID: 6495

Remote: Yes

Date Published: Dec 30 2002 12:00AM

Relevant URL:

<http://www.securityfocus.com/bid/6495>

Summary:

Microsoft Visual SourceSafe is software to manage development projects in any programming language.

Microsoft Visual SourceSafe performs validation of permissions for access control for projects on the client side, instead of on the server side.

This poses a security threat because a malicious client user may potentially circumvent these security measures to gain unauthorized access to protected files within a project. The only way to restrict access on the server side is to set NTFS permissions, but these permissions must reportedly be applied to an entire project and not individual project files or folders.

If an attacker can exploit this weakness, it will be possible to gain unauthorized access to restricted files within projects that the attacker has access to. As a consequence, it may be possible for a malicious user to view or modify sensitive data in project files. This has the potential to violate security policy for development projects.

8. PHP wordwrap() Heap Corruption Vulnerability

BugTraq ID: 6488

Remote: Yes

Date Published: Dec 27 2002 12:00AM

Relevant URL:

<http://www.securityfocus.com/bid/6488>

Summary:

PHP is a freely available, open source web scripting language package. It is available for Microsoft Windows, Linux, and Unix operating systems.

A vulnerability has been discovered in the wordwrap() function which is a built-in PHP function. Under some circumstances it may be possible to trigger a heap corruption bug when supplying input to a script which uses the vulnerable wordwrap() function. This issue exists due to insufficient

allocation of memory used to store wrapped text. Memory corrupted through the wordwrap() function may be later referenced by the web server calling the vulnerable script.

A malicious attacker may be able to exploit this issue to overwrite a malloc header stored in the heap. This may cause an arbitrary word in memory to be overwritten when corrupted chunk is released with the free() function. By replacing a Global Offset Table entry with an address pointed to attacker-supplied data, it may be possible for the attacker to execute malicious instructions. Any code executed will be run with the privileges of the web server that ran the vulnerable script.

9. Gallery Remote Code Execution Vulnerability

BugTraq ID: 6489

Remote: Yes

Date Published: Dec 28 2002 12:00AM

Relevant URL:

<http://www.securityfocus.com/bid/6489>

Summary:

Gallery is an open source web based photo album. It is written in PHP and is available for Linux and Unix variant as well as Microsoft Windows operating systems.

A new feature supporting the Windows XP publishing subsystem in Gallery 1.3.2 has introduced a security vulnerability nearly identical to that described in BID 5375.

The PHP script 'publish_xp_docs.php' attempts to include a file, 'init.php', from a path constructed using an uninitiated PHP variable. Malicious remote clients may pass a value for that variable, specifying a remote server as the location of the include file. By doing so, attackers may force a remote server to execute arbitrary PHP code with the privileges of the webserver.

III. MICROSOFT FOCUS LIST SUMMARY

1. Account Management (Thread)

Relevant URL:

<http://online.securityfocus.com/archive/88/305008>

2. SecurityFocus Microsoft Newsletter #119 (Thread)

Relevant URL:

<http://online.securityfocus.com/archive/88/304736>

3. MDAC 2.7 SP1 now available as a standalone install (Thread)

Relevant URL:

<http://online.securityfocus.com/archive/88/304675>

IV. NEW PRODUCTS FOR MICROSOFT PLATFORMS

1. East-Tec FormatSecure

by EAST Technologies

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

<http://www.east-tec.com/erprod/formatsc/index.htm>

Summary:

East-Tec FormatSecure, in addition to formatting the drive, will securely wipe the entire contents of the drive in order to stop software and hardware tools from recovering any data. East-Tec FormatSecure is a component of our family of products designed for the entire family of Windows operating systems (Windows 95/98/Me/NT/2000/XP) to completely eliminate sensitive data from your computer.

2. KillDisk

by LSoft Technologies Inc.

Platforms: DOS, Linux, UNIX, Windows 2000, Windows 95/98, Windows NT, Windows XP

<http://www.killdisk.com/eraser.htm>

Summary:

Active@ Kill Disk is disk eraser software for secure formatting of hard drives without any possibility of following data recovery. DOS application can be run from floppy boot disk. Eraser uses access to drive's data on physical level via BIOS bypassing logical drive structure organization, thus it formats disk bypassing operating systems and file systems located on IBM PC. DoD 5220.22-M compatible.

3. Norton SystemWorks 2003

by Symantec

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

<http://www.symantec.com/sabu/sysworks/basic/>

Summary:

Symantec's Norton SystemWorks? 2003 is the smartest way to solve computer problems. It includes award-winning Symantec products and additional utilities that help you protect your PC from virus threats, optimize performance, fix and prevent problems, recover from system failures, clean out Internet clutter, and keep dial-up connections active when you're online.

V. NEW TOOLS FOR MICROSOFT PLATFORMS

1. DumpWin v2.0

by Network Intelligence India Pvt. Ltd.

Relevant URL:

<http://www.nii.co.in/tools.html>

Platforms: Windows 2000, Windows NT, Windows XP

Summary:

Dumpwin is a windows data gathering tool, which includes the functionality of the tool DumpACL. In addition, DumpWin also gathers information about the system, users, groups, drives, shares, running processes, installed software, installed hardware, services, open ports, etc. It also dumps the ACLs of user-specified files/folders and registry keys. It is useful for auditors to dump all relevant data from a Windows system.

2. AnalogX Script Defender 1.01

by AnalogX mark@analogx.com

Relevant URL:

<http://www.analogx.com/files/sdefendi.exe>

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

Summary:

AnalogX Script Defender will intercept any request to execute the most common scripting types used in virus attacks, such as Visual Basic Scripting (.VBS), Java Script (.JS), etc and can even be configured to intercept new script extensions as needed. It's very simple to use and helps to ensure that you do not inadvertently run a script no matter what email program you use, or even if you get it via another method.

3. pcInternet Patrol

by Internet Security Alliance

Relevant URL:

<http://www.isa-llc.com/downloads/pcip.php>

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

Summary:

pcInternet Patrol maximizes protection with minimum user involvement This product finds 6 times more potentially dangerous programs/modules than other leading personal firewalls. Other features are:

- Stops all intruder programs both known and unknown;
- Users always have the latest programs definition without the need for an update;
- Keeps you and your computer out of harms way, without getting in your way;
- Cannot be disabled by an intruder without alerting user or administrator;
- Activates Intruder tracking to trace IP address of intruder for possible apprehension;
- Continuously monitors the state of the NETBIOS ports, the first entry target for intruders;
- Help with security issues in real time!

VI. SPONSOR INFORMATION

This issue is sponsored by: Qualys

Strengthening Network Security: FREE Guide Network security is a constantly moving target – even proven solutions lose their punch over time. Find out how to get COMPLETE PROTECTION against ever-growing

SecurityFocus Microsoft: SecurityFocus Microsoft Newsletter #120

security threats with our FREE new Guide.

Get your copy today at: https://www.qualys.com/forms/nsguideh_376.php
