

SecurityFocus Microsoft Newsletter #152

Source: <http://www.derkeiler.com/Mailing-Lists/securityfocus/focus-ms/2003-09/0038.html>

From: Marc Fossi (mfossi_at_securityfocus.com)

Date: 09/08/03

Date: Mon, 8 Sep 2003 08:47:08 -0600 (MDT)

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

SecurityFocus Microsoft Newsletter #152

This Issue is Sponsored by: Foundstone

FREE Trial! New for security consultants and in-house pros: FOUNDSTONE PROFESSIONAL and PROFESSIONAL TL software. Fast, reliable vulnerability assessment technology powered by the award-winning FoundScan engine. Try it free for 21 days at:

http://www.securityfocus.com/sponsor/Foundstone_ms-secnews_030902

I. FRONT AND CENTER

1. Pocket-Sized Wireless Detection

II. MICROSOFT VULNERABILITY SUMMARY

1. Real Networks Helix Universal Server Remote Buffer Overflow ...
2. IdealBB HTML Injection Vulnerability
3. Castle Rock Computing SNMPc v5/v6 Unauthorized Remote Privil...
4. AnalogX Proxy DNS Lookup Error Page Cross-Site Scripting Vul...
5. newsPHP Remote File Include Vulnerability
6. newsPHP Authentication Bypass Vulnerability
7. Attila PHP SQL Injection Unauthorized Privileged Access Vuln...
8. Tellurian TftpdNT Long Filename Buffer Overrun Vulnerability
9. WorldFlash News Ticker Remote Buffer Overrun Vulnerability

III. MICROSOFT FOCUS LIST SUMMARY

1. focus-ms@securityfocus.com (Thread)
2. Administrivia: lost messages sent since Wednesday (Thread)
3. Patch testing (Thread)
4. SecurityFocus Microsoft Newsletter # 151 (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. ccrypt v1.6
2. Star v1.5a21
3. Password Manager XP v1.5
4. beecrypt v3.1.0
5. Anti-Spam SMTP Proxy v1.0.0
6. ngrep v1.41

VI. SPONSOR INFORMATION

I. FRONT AND CENTER

1. Pocket-Sized Wireless Detection

By Bob Rudis

This article provides a comparison of two tiny 802.11 detectors and discusses how they would fit into your overall WiFi security framework.

<http://www.securityfocus.com/infocus/1727>

II. MICROSOFT VULNERABILITY SUMMARY

1. Real Networks Helix Universal Server Remote Buffer Overflow ...

BugTraq ID: 8476

Remote: Yes

Date Published: Aug 22 2003

Relevant URL: <http://www.securityfocus.com/bid/8476>

Summary:

Helix Universal Server is a multiple type media server distributed and maintained by Real Networks. It is available for Unix, Linux, and Microsoft Windows platforms.

Real Networks has announced that a vulnerability is present in Helix Universal Server version 9 and prior that will allow for attackers to remotely compromise servers. The condition occurs when URLs containing an excessive number of './.' sequences are sent to the Server's protocol parsers. A remote attacker may pass a malicious request that is sufficient to overflow a 1024 byte buffer on the stack. Ultimately the attacker may influence execution flow into attacker controlled heap based memory. This will result in arbitrary attacker supplied instructions being executed in the context of the affected Helix server.

The vulnerability is reportedly present in the "View Source" plug-in and may be eliminated if the plug-in is disabled. The plug-in is used for reading and displaying file format header information of files accessible on the server filesystem. It also supports the "Content Browsing" feature, which will not function if the plug-in is disabled. Additionally, disabling the plug-in will not adversely affect on-demand or live streaming delivery or the logging and authentication services of the server.

It has been reported that exploitation of this issue is hindered somewhat on SPARC systems or other systems that are word aligned.

Note: The announcement by RealNetworks may be related to issues reported earlier by Symantec (possibly BIDs 7020, 6454, 6458 or 6456). This has not been confirmed. However, if this is indeed the case, this BID will be retired.

2. IdealBB HTML Injection Vulnerability

BugTraq ID: 8480

Remote: Yes

Date Published: Aug 23 2003

Relevant URL: <http://www.securityfocus.com/bid/8480>

Summary:

IdealBB is a web based bulletin board system implemented in ASP. It runs on Microsoft Windows platforms using SQL Server on the back end.

IdealBB is prone to a script injection issue. The software allows raw HTML to be inserted into messages. The software then strips any script code from the embedded HTML.

The problem occurs because IdealBB fails to strip script code containing HTML entities in place of certain characters. Any script code inserted using this method would be executed in the web browser of the user viewing the malicious message.

3. Castle Rock Computing SNMPc v5/v6 Unauthorized Remote Privil...

BugTraq ID: 8484

Remote: Yes

Date Published: Aug 25 2003

Relevant URL: <http://www.securityfocus.com/bid/8484>

Summary:

SNMPc is a Distributed Network Manager developed and maintained by Castle Rock Computing. SNMPc is available for the Microsoft Windows operating system. For monitoring and administering the SNMPc server, the product includes a remote console, which is accessible to authenticated remote users.

It has been discovered that all authentication routines, when connecting to the aforementioned console, are carried out within the client program. Specifically, when an authentication request to the server is made, user data will be transmitted from the server to the client, this data includes an encrypted password. This password is compared client-side, to the password that is supplied; if successful the client likely transmits a packet to the server notifying it of a successful authentication.

An attacker could exploit this issue in one of two ways. First, it has been reported that the encryption scheme used to obfuscate the password transmitted by the server, is no more than a simple substitution cipher, making it trivial for an attacker to deduce the plaintext. Second, it may be possible for an attacker to reverse and modify specific components of a

client program, and thus influence it's behavior in such a way that authentication may be granted when the routine actually failed.

Ultimately, this issue could allow an attacker to reveal users passwords, such as the 'Administrator' user, who has 'Supervisor' privileges by default. Or gain unauthorized console access, with 'Supervisor' privileges on a target server, without supplying a password at all.

It should be noted that the 'Administrator' user cannot be deleted or modified.

Privileged access to a remote console on a target server may allow an attacker to gain sensitive information which could be used in later attacks, or modify the behavior of an administered network, etc.

This vulnerability affects SNMPc v5 and version v6.

4. AnalogX Proxy DNS Lookup Error Page Cross-Site Scripting Vul...

BugTraq ID: 8487

Remote: Yes

Date Published: Aug 25 2003

Relevant URL: <http://www.securityfocus.com/bid/8487>

Summary:

AnalogX Proxy is proxy server software for Microsoft Windows operating systems. It supports various protocols including HTTP.

The AnalogX Proxy is prone to a cross-site scripting issue that can be exploited through error pages.

When a DNS lookup for a domain fails, AnalogX Proxy returns an error page including the failed URL. If any script code is included in this failed URL, it will be executed in the client web browser.

This issue allows a user to be prone to attacks such as cookie-based credential theft. Other attacks may also be possible.

5. newsPHP Remote File Include Vulnerability

BugTraq ID: 8488

Remote: Yes

Date Published: Aug 25 2003

Relevant URL: <http://www.securityfocus.com/bid/8488>

Summary:

newsPHP is a web-based content management system. It is implemented in PHP and is available for a variety of platforms including Microsoft Windows and Linux variant operating systems.

newsPHP is reported to be prone to a vulnerability that may allow remoter attackers to include files containing arbitrary code to be executed on a host running the vulnerable software. This issue is exploitable via the LangFile variable of nphpd.php module. It has been reported that the LangFile variable is not set by default in newPHP and may be exploited by

influencing its path to point to a malicious file supplied by the attacker.

This vulnerability may lead to execution of arbitrary code by an attacker in the form of PHP commands in the context of the web server hosting the vulnerable version of newsPHP.

newsPHP v216 is reported to be vulnerable to this issue, however other versions may be affected as well.

6. newsPHP Authentication Bypass Vulnerability

BugTraq ID: 8489

Remote: Yes

Date Published: Aug 25 2003

Relevant URL: <http://www.securityfocus.com/bid/8489>

Summary:

newsPHP is a web-based content management system. It is implemented in PHP and is available for a variety of platforms including Microsoft Windows and Linux variant operating systems.

It has been reported that newsPHP contains an authentication bypass vulnerability allowing an unauthenticated attacker to gain access to sensitive data or perform unauthorized actions. The issue occurs due to the failure of newPHP to check authentication credentials of a remote user. An attacker may send a request to perform an action via a specially crafted URI containing illegitimate authentication credentials in order to gain access to sensitive data.

The issue is reported to exist in newPHP v216, however other versions may be affected as well.

7. Attila PHP SQL Injection Unauthorized Privileged Access Vuln...

BugTraq ID: 8502

Remote: Yes

Date Published: Aug 26 2003

Relevant URL: <http://www.securityfocus.com/bid/8502>

Summary:

Attila PHP is a PHP content management system designed for portal sites. It is available for Unix, Linux, and Microsoft Windows platforms.

An SQL injection vulnerability has been reported in Attila PHP that could allow an attacker to gain unauthorized privileged access to a target site. The problem occurs due to Attila PHP failing to sufficiently encapsulate the 'cook_id' variable within quotes. As a result, an attacker may inject SQL commands within the variable, and influence the result of an SQL query carried out by the program. This could ultimately allow an attacker to be granted access to the site as an arbitrary user, possibly an administrator.

Privileged access to a site implementing Attila PHP could allow an attacker to reveal or modify sensitive information or potentially launch

other attacks. It should be noted that, although unconfirmed it may be possible for an attacker to injection SQL commands into the query that could aid in launching attacks against the underlying database.

This vulnerability is said to affect Attila PHP 3.0.

8. Tellurian TftpdNT Long Filename Buffer Overrun Vulnerability

BugTraq ID: 8505

Remote: Yes

Date Published: Aug 27 2003

Relevant URL: <http://www.securityfocus.com/bid/8505>

Summary:

Tellurian TftpdNT is a typical RFC compliant TftpdNT server for the Microsoft Windows operating system.

It has been discovered that some versions of Tellurian TftpdNT may be prone to a buffer overrun vulnerability. The problem is believed to occur due to insufficient bounds checking when handling user-supplied filenames. As a result, handling a filename of excessive length may result in unexpected data being written to memory adjacent to the filename buffer.

This could potentially corrupt sensitive stack variables such as function pointers, saved frame pointers, or return addresses. As a result, an attacker may be capable of seizing control of a target TftpdNT server by passing it a specially formatted filename. This could ultimately result in the execution of arbitrary code, with the privileges of TftpdNT.

This vulnerability is said to affect Tullerian TftpdNT 2.0 and earlier.

9. WorldFlash News Ticker Remote Buffer Overrun Vulnerability

BugTraq ID: 8511

Remote: Yes

Date Published: Aug 28 2003

Relevant URL: <http://www.securityfocus.com/bid/8511>

Summary:

World Flash News Ticker is a program designed to collect various news events and display them to the user. It can be customized to access specific links, etc. It is available for the Microsoft Windows operating system.

A buffer overrun vulnerability has been alleged in WorldFlash News Ticker. The problem is said to occur when receiving HTML data from remote sites. This problem likely occurs due to insufficient bounds checking, and could potentially be exploited by a remote host to trigger the execution of arbitrary code. It should be noted that the remote host would likely have to be on a list of links that the affected product references for news items.

This vulnerability is said to affect WorldFlash News Ticker Gold M5.30i, however, other versions may also be affected.

III. MICROSOFT FOCUS LIST SUMMARY

1. focus–ms@securityfocus.com (Thread)

Relevant URL:

<http://www.securityfocus.com/archive/88/335653>

2. Administrivia: lost messages sent since Wednesday (Thread)

Relevant URL:

<http://www.securityfocus.com/archive/88/335344>

3. Patch testing (Thread)

Relevant URL:

<http://www.securityfocus.com/archive/88/335245>

4. SecurityFocus Microsoft Newsletter # 151 (Thread)

Relevant URL:

<http://www.securityfocus.com/archive/88/334869>

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. 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.

2. 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.

3. Password Manager XP v1.5

By: CP-Lab

Relevant URL: <http://www.cp-lab.com>

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

Summary:

Password Manager XP is a program that helps you to systematize any secret information stored on your PC. It will be your passwords and secrets keeper. Protect your private data with this password management utility. Password Manager XP allows you to create several databases for storing your secret information. Each database has an access password and is encrypted with various algorithms at the same time (Blowfish, 3DES, Rijndael, Tea, Cast128, RC4, Serpent, Twofish). You can store data in different databases under your own passwords. You can create passwords databases at shared resource and access them from multiple computers across the network. Install to removable device Wizard will help you to install the Password Manager XP to the removable devices such a USB flash drives. It is easily integrated into Microsoft Internet Explorer. It helps you to surf the Web more safely. Password Manager XP has a built-in password generator with many adjustable functions.

4. beecrypt v3.1.0

By: Bob Deblie, bob.deblie@pandora.be

Relevant URL: <http://sourceforge.net/projects/beecrypt/>

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

Summary:

BeeCrypt is an ongoing project to provide strong and fast cryptography in the form of a toolkit usable by commercial and open source projects. Included in the library are entropy sources, random generators, block ciphers, hash functions, message authentication codes, multiprecision integer routines, and public key primitives.

5. Anti-Spam SMTP Proxy v1.0.0

By: John Hanna

Relevant URL: <http://assp.sourceforge.net/>

Platforms: BSDI, Linux, MacOS, Os Independent, OS/2, Perl (any system supporting perl), POSIX, Windows 2000, Windows NT

Summary:

The Anti-Spam SMTP Proxy (ASSP) Server project aims to create an open source platform independent SMTP Proxy server which implements whitelists and Bayesian filtering to help stop unsolicited commercial email (UCE). Anti-spam tools should be adaptive to new spam and customized for each site's email patterns. This easy to use tool works with any mail transport and achieves these goals requiring no operator intervention after the initial setup phase.

6. ngrep v1.41

By: Jordan Ritter <jpr5@darkridge.com>

Relevant URL: <http://ngrep.sourceforge.net/>

Platforms: AIX, Digital UNIX/Alpha, FreeBSD, IRIX, Linux, OpenBSD, Solaris, Windows 2000, Windows 95/98, Windows NT

Summary:

ngrep strives to provide most of GNU grep's common features, applying them to the network layer. ngrep a pcap-aware tool that will allow you to specify extended regular expressions to match against data payloads of packets. It currently recognizes TCP and UDP across ethernet, ppp and slip interfaces, and understands bpf filter logic in the same fashion as more common packet sniffing tools like tcpdump and snoop.

VI. SPONSOR INFORMATION

This Issue is Sponsored by: Foundstone

FREE Trial! New for security consultants and in-house pros: FOUNDSTONE PROFESSIONAL and PROFESSIONAL TL software. Fast, reliable vulnerability assessment technology powered by the award-winning FoundScan engine. Try it free for 21 days at:

http://www.securityfocus.com/sponsor/Foundstone_ms-secnews_030902

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
