

SecurityFocus Microsoft Newsletter #164

Source: <http://www.derkeiler.com/Mailing-Lists/securityfocus/focus-ms/2003-11/0132.html>

From: Marc Fossi (mfossi_at_securityfocus.com)

Date: 11/24/03

Date: Mon, 24 Nov 2003 14:58:55 -0700 (MST)

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

SecurityFocus Microsoft Newsletter #164

This issue is sponsored by: NeoScale – Enterprise Storage Security that's Simple, Reliable Secure.

Got Storage Security Risks? Consolidation, Continuity, Compliance Connected, accessible and distributed storage can enable unauthorized access to sensitive, trusted and regulated information. What are best storage security practices? Discover how to alleviate exposures within shared and managed storage, disaster recovery, vaulting, as well as auditing and compliance processes. Obtain your FREE whitepaper from NeoScale at

http://www.securityfocus.com/sponsor/NeoScale_ms-secnews_031124

I. FRONT AND CENTER

1. Home User Security: Your First Defense

II. MICROSOFT VULNERABILITY SUMMARY

1. NetServe Web Server Directory Traversal Vulnerability
2. PostgreSQL 7.4 Release To Fix Several Security Vulnerabiliti...
3. Kerio WinRoute Firewall Authentication Credentials Exposure ...
4. Yak! Chat Client FTP Server Default Username Credential Weak...
5. EffectOffice Server Remote Service Buffer Overflow Vulnerabi...
6. Sybase Adaptive Server Remote Password Array Heap Overflow V...

III. MICROSOFT FOCUS LIST SUMMARY

1. TechNet Security Webcast Week (Thread)
2. iis – authenticate thru domain username/password (Thread)
3. Hiding MS SQL databases in Enterprise Manager (Thread)
4. IIS traffic (Thread)
5. Strange behaviour of MS SQL 2000 (Thread)
6. MS03-049 Scanner? (Thread)
7. MS03-049 Vulnerability (Thread)
8. SecurityFocus Microsoft Newsletter #163 (Thread)

IV. NEW PRODUCTS FOR MICROSOFT PLATFORMS

1. EnCase Enterprise Edition
2. SafeGuard PDA
3. The CyberAngel Security Software
4. Cyber-Ark Inter-Business Vault

5. EnCase Forensic Edition

6. OverflowGuard

V. NEW TOOLS FOR MICROSOFT PLATFORMS

1. Stealth HTTP Security Scanner v2.0b36

2. aNTG v2.0

3. Logrep v1.4.2

4. OSIRIS v2.1.0

5. Glub Tech Secure FTP v2.0.11

6. Enigmail v0.82.0

VI. SPONSOR INFORMATION

I. FRONT AND CENTER

1. Home User Security: Your First Defense

By Sarah Granger

This article focuses on protecting the home office through personal firewall software, as well as general security measures that are often overlooked by home users.

<http://www.securityfocus.com/infocus/1746>

II. MICROSOFT VULNERABILITY SUMMARY

1. NetServe Web Server Directory Traversal Vulnerability

BugTraq ID: 9059

Remote: Yes

Date Published: Nov 17 2003

Relevant URL: <http://www.securityfocus.com/bid/9059>

Summary:

NetServe Web Server is a compact web server for Microsoft Windows platforms.

A vulnerability has been reported to exist in the software that may allow a remote attacker to access information outside the server root directory. The problem exists due to insufficient sanitization of user-supplied data. The issue may allow a remote attacker to traverse outside the server root directory by using '../' character sequences. It has been reported that this issue could be exploited to gain access to configuration files and harvest administrator login and password information.

Successful exploitation of this vulnerability may allow a remote attacker to gain access to sensitive information that may be used to launch further attacks against a vulnerable system.

NetServe Web Server version 1.0.7 is reported to be prone to this issue, however other versions may be affected as well.

2. PostgreSQL 7.4 Release To Fix Several Security Vulnerabiliti...

BugTraq ID: 9066

Remote: Yes

Date Published: Nov 18 2003

Relevant URL: <http://www.securityfocus.com/bid/9066>

Summary:

PostgreSQL is a freely distributed Object-Relational DBMS. It is available for a number of platforms including Unix and Linux variants and Microsoft Windows operating systems.

The PostgreSQL development group has reported the release of PostgreSQL version 7.4. This release contains feature and security enhancements.

The release also contains fixes for several potential security vulnerabilities. Issues fixed in this release include a contributed fix for a condition where an ampersand character in an XML document could trigger a violation in the PostgreSQL server and cause it to crash. This issue may be exploited to deny service to legitimate PostgreSQL users.

Additionally, a fix has been implemented that is designed to address a condition where users without sufficient privileges may potentially disable server log variables/logging that were added or enabled by the administrator. An attacker may potentially exploit this condition to hide malicious activity.

This BID will be updated as further details regarding these vulnerabilities are disclosed.

3. Kerio WinRoute Firewall Authentication Credentials Exposure ...

BugTraq ID: 9071

Remote: Yes

Date Published: Nov 19 2003

Relevant URL: <http://www.securityfocus.com/bid/9071>

Summary:

Kerio WinRoute Firewall is an enterprise level firewall that is also capable of proxying networks. It is available for the Microsoft Windows operating system.

If the WinRoute software has been configured as a proxy and authentication has been enabled, each time a web request is made from an internal host the client browser will include the Proxy-Connection HTTP header field. This value of this field will contain a Base64 encoded username and password, allowing the users request to be transmitted to the intended host.

A vulnerability has been discovered in WinRoute when acting as an authenticating proxy that could result in the exposure of authentication credentials. The problem lies in the fact that the software fails to sufficiently rebuild HTTP requests containing Proxy-Connection fields. The application simply replaces the first character of the field (P) with an X, and forwards the request to its intended destination. Because this field contains the aforementioned encoded credentials, a malicious web site administrator may be capable of parsing incoming HTTP requests for "Xroxy-Connection" and harvesting users proxy authentication credentials.

Access to these credentials could allow an attacker to carry out some form of attack on the proxy or possibly use the proxy as a means to hide the origin of attacks against unrelated hosts.

It should be noted that the exposure of user credentials is exaggerated by the fact that users are often known to use identical authentication credentials across varying services.

This vulnerability is reported to affected Kerio WinRoute Firewall 5.10, however other versions may also be affected.

4. Yak! Chat Client FTP Server Default Username Credential Weak...

BugTraq ID: 9072

Remote: Yes

Date Published: Nov 19 2003

Relevant URL: <http://www.securityfocus.com/bid/9072>

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 weakness exists in the Yak! client FTP server. This problem may increase the chances of an attacker gaining unauthorized access to resources.

The problem is in the default username credential created with the Yak! FTP server. When the FTP server is installed, it installs a user 'y049575046' with a potentially predictable password string 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.

5. EffectOffice Server Remote Service Buffer Overflow Vulnerabi...

BugTraq ID: 9077

Remote: Yes

Date Published: Nov 20 2003

Relevant URL: <http://www.securityfocus.com/bid/9077>

Summary:

EffectOffice Server is a commercially available office software infrastructure. It is available for the Microsoft Windows platform.

A problem has been reported in the service used by EffectOffice Server. Because of this, it may be possible for a remote user to deny service to legitimate users of the software.

EffectOffice Server launches a process that listens for inbound TCP connections on port 56004. However, when an attacker remotely connects to the service and sends strings of excessive length, the service becomes unstable and crashes. The service requires a manual restart to resume normal operations.

This problem is likely a boundary condition error, though no conclusive proof exists at this time. If this is the case, it could be possible for

a remote attacker to execute code with the privileges of the EffectOffice Server process.

6. Sybase Adaptive Server Remote Password Array Heap Overflow V...
BugTraq ID: 9080

Remote: Yes

Date Published: Nov 20 2003

Relevant URL: <http://www.securityfocus.com/bid/9080>

Summary:

Sybase Adaptive Server is a full SQL relational database management system. It is available for a variety of platforms including Microsoft Windows operating systems.

Sybase adaptive server has been reported prone to heap overflow vulnerability. The issue has been reported to present itself when invalid password and servername buffer lengths in a remote password array are passed to the affected server. A heap overflow condition may be triggered, potentially causing heap memory management structures to be corrupted.

It has been reported that an attacker may exploit this vulnerability to trigger a denial of service condition. The impact of this denial of service differs depending on the platform that the Adaptive Server is installed.

On a Windows platform a single successful exploit attempt on a client thread, will cause the server to cease to negotiate login attempts and will additionally prevent the server from responding to all commands.

On a Linux platform the exploited client process will crash, but other clients and the server process will remain unaffected. However the attacker may exploit the issue in quick succession and in doing so may potentially prevent clients from successfully negotiating Adaptive Server login attempts.

It has been conjectured that due to the nature of this vulnerability an exploit may be written that manipulates heap management structures in a manner that is sufficient so that remote arbitrary code execution occurs, this however has not been confirmed.

III. MICROSOFT FOCUS LIST SUMMARY

1. TechNet Security Webcast Week (Thread)

Relevant URL:

<http://www.securityfocus.com/archive/88/345408>

2. iis – authenticate thru domain username/password (Thread)

Relevant URL:

<http://www.securityfocus.com/archive/88/345407>

3. Hiding MS SQL databases in Enterprise Manager (Thread)

Relevant URL:

<http://www.securityfocus.com/archive/88/345406>

4. IIS traffic (Thread)

Relevant URL:

<http://www.securityfocus.com/archive/88/345405>

5. Strange behaviour of MS SQL 2000 (Thread)

Relevant URL:

<http://www.securityfocus.com/archive/88/345403>

6. MS03-049 Scanner? (Thread)

Relevant URL:

<http://www.securityfocus.com/archive/88/344925>

7. MS03-049 Vulnerability (Thread)

Relevant URL:

<http://www.securityfocus.com/archive/88/344924>

8. SecurityFocus Microsoft Newsletter #163 (Thread)

Relevant URL:

<http://www.securityfocus.com/archive/88/344817>

IV. NEW PRODUCTS FOR MICROSOFT PLATFORMS

1. EnCase Enterprise Edition

By: Guidance Software Inc.

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

Relevant URL: http://www.guidancesoftware.com/frame_encase.html

Summary:

EnCase, a computer forensic tool, is Windows– based and fully integrated. A tool that allows an investigator to conduct a complete, non–invasive forensic investigation from start to finish. This tool is used by law enforcement and has been accepted and authenticated in hundreds of court cases.

2. SafeGuard PDA

By: Utimaco

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

Relevant URL: http://www.utimaco.com/content_products/sg_pda.html

Summary:

SafeGuard PDA is a powerful solution to protect your Personal Digital Assistant and the data stored on it against unauthorized access. Whether the Pocket PC is for private use or a part of the company network, it requires at least the same degree of protection as notebooks and workstations. Since overall security is only as strong as the weakest link, SafeGuard PDA is the next logical step towards securing your mobile work force. Innovative authentication mechanisms such as biometric signature recognition or Symbol PIN offer optimal user convenience, the strong encryption protects your data while stored or in transit over the Internet, the centrally enforceable security policy keeps your environment consistently protected.

3. The CyberAngel Security Software

By: CyberAngel Security Solutions, Inc.

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

Relevant URL: <http://www.thecyberangel.com/ca-secure.html>

Summary:

The CyberAngel Security Software, a comprehensive approach to providing security for your laptop or desktop computer.

The CyberAngel Security Software utilizes our patented technology to Alert, Lock and Locate in the event of an unauthorized access of a computer.

4. Cyber-Ark Inter-Business Vault

By: Cyber-Ark

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

Relevant URL:

http://www.cyber-ark.com/datasecuritysoftware/inter-business_vault.htm

Summary:

Based on Cyber-Ark Software's Vaulting Technology, the Inter-Business Vault, an information security solution that enables organizations to safely overcome traditional network boundaries in order to securely share business information among customers, business partners, and remote branches. It provides a seamless, LAN-like experience over the Internet that includes all the security, performance, accessibility, and ease of administration required to allow organizations to share everyday information worldwide. To learn more about these core attributes of the Inter-Business Vault click on the relevant link below:

5. EnCase Forensic Edition

By: Guidance Software Inc.

Platforms: DOS, FreeBSD, Linux, MacOS, NetBSD, OpenBSD, PalmOS, Solaris, UNIX, Windows 2000, Windows 95/98, Windows NT, Windows XP

Relevant URL:

<http://www.guidancesoftware.com/products/EnCaseForensic/index.shtm>

Summary:

EnCase Forensic Edition Version 4 delivers the most advanced features for computer forensics and investigations. With an intuitive GUI and superior performance, EnCase Version 4 provides investigators with the tools to conduct large-scale and complex investigations with accuracy and efficiency. Guidance Software's award winning solution yields completely non-invasive computer forensic investigations while allowing examiners to easily manage large volumes of computer evidence and view all relevant files, including "deleted" files, file slack and unallocated space.

The integrated functionality of EnCase allows the examiner to perform all functions of the computer forensic investigation process. EnCase's EnScript, a powerful macro-programming language and API included within EnCase, allows investigators to build customized and reusable forensic scripts.

6. OverflowGuard

By: DATA Security Software

Platforms: Windows 2000, Windows NT, Windows XP

Relevant URL: <http://www.datasecuritysoftware.com/index.html>

Summary:

OverflowGuard provides stack and heap buffer overflow protection for services running under Windows NT4, 2000, XP and 2003.

V. NEW TOOLS FOR MICROSOFT PLATFORMS

1. 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.

2. aNTG v2.0

By: Lucas

Relevant URL: <http://www.thebobo.com/antg.php>

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

Summary:

aNTG (another Network Traffic Grapher) is a PHP program that collects and graphs network traffic statistics on a Linux machine.

3. Logrep v1.4.2

By: Tevfik Karagülle

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

Platforms: Linux, POSIX, Windows 2000, Windows NT

Summary:

Logrep is a secure multi–platform framework for the collection, extraction, and presentation of information from various log files. It features HTML reports, multi–dimensional analysis, overview pages, SSH communication, and graphs, and supports more than 15 popular systems including Snort, Squid, Postfix, Apache, syslog, iptables/ipchains, NT event logs, Firewall–1, wtmp, Oracle listener, and Pix.

4. OSIRIS v2.1.0

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).

5. Glub Tech Secure FTP v2.0.11

By: glub

Relevant URL: <http://secureftp.glub.com>

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

Summary:

Glub Tech Secure FTP is a command–line utility that allows FTP connections to be made using SSL.

6. Enigmail v0.82.0

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.

VI. SPONSOR INFORMATION

This issue is sponsored by: NeoScale – Enterprise Storage Security that's Simple, Reliable Secure.

Got Storage Security Risks? Consolidation, Continuity, Compliance Connected, accessible and distributed storage can enable unauthorized access to sensitive, trusted and regulated information. What are best storage security practices? Discover how to alleviate exposures within shared and managed storage, disaster recovery, vaulting, as well as auditing and compliance processes. Obtain your FREE whitepaper from NeoScale at

http://www.securityfocus.com/sponsor/NeoScale_ms-secnews_031124
