

SecurityFocus Microsoft Newsletter #165

Source: <http://www.derkeiler.com/Mailing-Lists/securityfocus/focus-ms/2003-12/0004.html>

From: Marc Fossi (*mfossi_at_securityfocus.com*)

Date: 12/01/03

Date: Mon, 1 Dec 2003 15:54:24 -0700 (MST)

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

SecurityFocus Microsoft Newsletter #165

This Issue is Sponsored by: Tenable Security

Tenable provides security software which enables enterprises to distribute, manage, and communicate vulnerability and intrusion detection information across the entire organization. Tenable's breakthrough Lightning(tm) technology elegantly simplifies the complex nature of network security by offering detailed useable reports for network and security administrators and high-level organizational reports for CxOs. In addition, Tenable offers both active (NeWT) and passive (NeVO) vulnerability detection solutions to further enhance your network vulnerability identification. For more information, Tenable can be reached at 410-872-0555 or on the Internet at http://www.securityfocus.com/sponsor/TenableSecurity_ms-secnews_031201

I. FRONT AND CENTER

1. Fighting Spammers With Honeypots: Part 1
2. Fighting Spammers With Honeypots: Part 2
3. The Wells Fargo Example
4. Exploiting Cisco Routers: Part 2

II. MICROSOFT VULNERABILITY SUMMARY

1. Microsoft MSN Messenger Information Leakage Weakness
2. Imatix Xitami Post Request Header Remote Denial Of Service V...
3. PrimeBase SQL Database Server Administrative Server Password...
4. Opera Skin Zip File Buffer Overflow Vulnerability
5. Qualcomm Eudora Attachment LaunchProtect Warning Bypass Weak...
6. HP ProCurve Switch Denial of Service Vulnerability
7. Microsoft Internet Explorer MHTML Forced File Execution Vuln...
8. Microsoft Internet Explorer Invalid ContentType Cache Direct...
9. Microsoft Internet Explorer Browser MHTML Redirection Local ...
10. Microsoft Internet Explorer Window.MoveBy/Method Caching Mou...
11. Microsoft Internet Explorer BackToFramedJPU Cross-Domain Pol...
12. Macromedia JRun Administrative Interface Multiple Cross-Site...
13. Microsoft Exchange Server 2003 Outlook Web Access Lowered Se...
14. phpBB search.php SQL Injection Vulnerability

III. MICROSOFT FOCUS LIST SUMMARY

1. are my binaries being exposed on my ASP.NET website? (Thread)
2. local admin account password (Thread)
3. how do I force secure ASP.NET session cookies? (Thread)
4. Strange behaviour of MS SQL 2000 (Thread)
5. IIS traffic (Thread)
6. SecurityFocus Microsoft Newsletter #164 (Thread)
7. Administrivia: Article Announcements (Thread)
8. TS group policy / hide notification area (Thread)
9. Article Announcement: Busting the Worm Writers (Thread)
10. Betr.: Strange behaviour of MS SQL 2000 (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. Generic Security Service v0.0.7
2. Enigmail v0.82.3
3. Stealth HTTP Security Scanner v2.0b36
4. aNTG v2.0
5. Logrep v1.4.2
6. OSIRIS v2.1.0

VI. SPONSOR INFORMATION

I. FRONT AND CENTER

1. Fighting Spammers With Honeypots: Part 1
By Laurent Oudot

This paper will evaluate the usefulness of using honeypots to fight spammers on several fronts. Part one discusses the methods spammers use to harvest addresses, maintain stealth and manipulate open mail relays on the Internet. Then honeypots will be considered that create fake email addresses to be harvested, identify and track spammers, and simulate open proxies for spammers to use.

<http://www.securityfocus.com/infocus/1747>

2. Fighting Spammers With Honeypots: Part 2
By Laurent Oudot

Part two continues the discussion of open proxies, describes creating fake open mail relays with various honeypots, discusses architecture decisions, and then provides some recent test results that proved very successful. A honeypot can clearly be used to detect, slow and stop spam-related activities while promoting a clean Internet — but more people must pitch in for them to truly make a difference.

<http://www.securityfocus.com/infocus/1748>

3. The Wells Fargo Example By Mark Rasch

Companies should protect consumer data better than Wells Fargo did, but in cleaning up its laptop data spill the bank blazed a trail worth following.

<http://www.securityfocus.com/columnists/201>

4. Exploiting Cisco Routers: Part 2 By Mark Wolfgang

This is the second of a two-part series that focuses on identifying and then exploiting vulnerabilities and poor configurations in Cisco routers. This article will look at what we can do once we've gotten in.

<http://www.securityfocus.com/infocus/1749>

II. MICROSOFT VULNERABILITY SUMMARY

1. Microsoft MSN Messenger Information Leakage Weakness

BugTraq ID: 9082

Remote: Yes

Date Published: Nov 20 2003

Relevant URL: <http://www.securityfocus.com/bid/9082>

Summary:

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

MSN Messenger is prone to an information leakage weakness. It has been reported that the problem exist in the MSN client during a file transfer invitation requests. The client improperly processes incoming requests and may send sensitive data such as the IP address of the client to the remote host without first identifying that host. The expected behavior is that the client must accept the file transfer prior to revealing its IP address. However, by exploiting this weakness, it is possible to obtain the client IP address prior to the client user accepting the file transfer request. This presents a security threat because it will allow an attacker to enumerate IP addresses of client users.

This information could be used to launch direct attacks against the client system and network.

MSN Messenger versions 6.0.0602 and prior and all versions of Windows Messenger have been reported to be prone to this issue. Other versions of MSN Messenger could be affected as well.

2. Imatix Xitami Post Request Header Remote Denial Of Service V...

BugTraq ID: 9083

Remote: Yes

Date Published: Nov 21 2003

Relevant URL: <http://www.securityfocus.com/bid/9083>

Summary:

Xitami is a freely available web server package distributed by Imatix. It is available for the Unix, Linux, and Microsoft platforms.

A problem has been identified in the handling of certain types of requests by Imatix Xitami. Because of this, it is possible for a remote attacker to deny service to legitimate users of a vulnerable server.

When an attacker crafts POST request with a header containing certain malformed fields, it is possible to force the Xitami server into an endless loop in execution. This typically results in the Xitami server crashing, resulting in a denial of service, and requiring a manual restart of the server to resume normal service.

3. PrimeBase SQL Database Server Administrative Server Password...

BugTraq ID: 9087

Remote: No

Date Published: Nov 22 2003

Relevant URL: <http://www.securityfocus.com/bid/9087>

Summary:

PrimeBase SQL Database Server is a database implementation that is available for Unix, Linux, and Microsoft Windows platforms.

A problem has been reported in the storage of credentials in PrimeBase SQL Database Server. Because of this, it may be possible for an attacker to gain unauthorized access to resources.

The problem is in the storage of authentication credentials. The administrative server included with PrimeBase SQL Database Server does not store authentication credentials in a secure format, keeping them in a plain text file. This problem is compounded by the fact that file is created with a default umask that permits world read access to the file.

This issue may permit an attacker with shell-level access to a system hosting the server to gain access to the database server administrative interface.

4. Opera Skin Zip File Buffer Overflow Vulnerability

BugTraq ID: 9089

Remote: Yes

Date Published: Nov 22 2003

Relevant URL: <http://www.securityfocus.com/bid/9089>

Summary:

Opera is a web browser available for a number of operating systems, including the Microsoft Windows, Linux, Unix, and Apple MacOS platforms.

A problem has been identified in the handling of zipped skin files by Opera. Because of this, it may be possible for an attacker to gain unauthorized access to a system using the vulnerable browser.

The problem is in the handling of specially crafted zip files. When a skin zip file with data appended after the zipped data is downloaded by Opera, the data contained after the zip data results in a boundary condition error. This could be exploited to overwrite sensitive process memory, potentially resulting in the modifying of program flow and execution of attacker-supplied instructions.

It should be noted that exploitation of this vulnerability may result in the execution of code with the privileges of the Opera browser user.

5. Qualcomm Eudora Attachment LaunchProtect Warning Bypass Weak...

BugTraq ID: 9101

Remote: Yes

Date Published: Nov 25 2003

Relevant URL: <http://www.securityfocus.com/bid/9101>

Summary:

Eudora is the freely available mail user agent (MUA) maintained and distributed by Qualcomm. It is available for the Microsoft Windows platform.

A problem has been identified in the implementation of LaunchProtect within Eudora. Because of this, it may be possible to trick users into performing dangerous actions.

The problem is in the handling of files outside of the LaunchProtect directory. When an attachment is saved inside the LaunchProtect directory, Eudora displays a warning message prior to opening any executable attachments. However, this is limited to the attach directory. An attachment placed outside of the attach directory would not prompt the warning from Eudora. This may lull the user into a false sense of security as they will not be cautioned about the attachment when opening it. The user would still need to interactively open the attachment.

The threat of this problem could be further increased by the issue described in Bugtraq ID 5432.

6. HP ProCurve Switch Denial of Service Vulnerability

BugTraq ID: 9103

Remote: Yes

Date Published: Nov 26 2003

Relevant URL: <http://www.securityfocus.com/bid/9103>

Summary:

A denial of service vulnerability has been reported to exist in the HP ProCurve Switches. The problem is reported to occur in the presence of RPC worms such as W32.Welchia.Worm (MCID 1811) and W32.Blaster.Worm (MCID 1761).

Reports have indicated that the vulnerable switches react in an unstable manner in the presence of certain RPC worms. This issue results in deteriorated network traffic leading to a denial of service condition for network users. This problem is reported to affect systems running

Microsoft Windows operating systems.

This vulnerability may cause the software to crash therefore denying service to legitimate users.

7. Microsoft Internet Explorer MHTML Forced File Execution Vuln...

BugTraq ID: 9105

Remote: Yes

Date Published: Nov 25 2003

Relevant URL: <http://www.securityfocus.com/bid/9105>

Summary:

A vulnerability has been discovered in Microsoft Internet Explorer when handling MHTML file URIs that may be exploited to download a malicious file to the client system and execute it if active content can be run in the Local Zone.

This issue involves using MHTML file and res URIs to redirect the browser into downloading an attacker-specified file. MHTML file URIs are used to specify the location of content embedded in an MHT file. MHTML URIs have the following format:

```
mhtml:[Mhtml_File_Uri]![Original_Resource_Uri]
```

It has been reported that if the resource specified in the Mhtml_File_Uri cannot be found, the browser will attempt to retrieve the resource specified in the Original_Resource_Uri.

The vulnerability can be exploited by setting the CODEBASE property of an OBJECT tag, using a previously unused CLSID, to a non-existent Mhtml_File_Uri and attacker-supplied Original_Resource_Uri. When the browser fails to retrieve the non-existent resource initially specified in the first part of the MHTML URI, it downloads content specified by the attacker instead in the second part of the URI. The content downloaded will subsequently be executed. This could be exploited in combination with other vulnerabilities such as those described in BID 9107 and 9109 to ultimately execute code within the Local Zone.

Due to the ease of exploitation and the existence of other vulnerabilities which may be exploited in tandem with this BID, it is probable that this issue will be widely exploited in the wild.

This issue was originally covered in BID 9100 "Multiple Internet Explorer Browser Security Model Compromise Vulnerabilities" and is now being assigned its own BID.

8. Microsoft Internet Explorer Invalid ContentType Cache Direct...

BugTraq ID: 9106

Remote: Yes

Date Published: Nov 25 2003

Relevant URL: <http://www.securityfocus.com/bid/9106>

Summary:

Microsoft Internet Explorer is prone to a weakness that may allow attackers to enumerate where cached Internet content is stored on the client filesystem. The attacker can exploit this by specifying an invalid ContentType in an HTTP response to the browser.

If the attacker can determine the location of cached content, it may be possible to reference this content using other known issues. This presents an attacker with the possibility of causing malicious active content to be stored in the cache and then referenced through exploitation of a number of other known issues in the browser. There are also existing issues in the browser that will allow this content to be interpreted in the context of the Local Zone (My Computer). This could be exploited in tandem with these other vulnerabilities from a malicious web page to cause code to be executed on a system running the vulnerable client.

Symantec has confirmed that this issue is exploitable on IE 5.0 as well as the version tested by the researcher. However, other external reports indicate difficulties reliably reproducing this issue on various versions of Microsoft Internet Explorer 6.0. This may have to do with particular browser and operation system settings. This BID will be updated if further information is made available to clarify which versions, patch levels and configurations are affected.

Due to the ease of exploitation and the existence of other vulnerabilities which may be exploited in tandem with this BID, it is probable that this issue will be widely exploited in the wild.

This issue was originally covered in BID 9100 "Multiple Internet Explorer Browser Security Model Compromise Vulnerabilities" and is now being assigned its own BID.

9. Microsoft Internet Explorer Browser MHTML Redirection Local ...

BugTraq ID: 9107

Remote: Yes

Date Published: Nov 25 2003

Relevant URL: <http://www.securityfocus.com/bid/9107>

Summary:

A vulnerability has been reported in Internet Explorer that may allow an attacker to parse local files on a system.

A vulnerability (MhtRedirParsesLocalFile) has been reported that may be exploited to cause Internet Explorer to parse a local file inside of an IFRAME. This vulnerability relies on use of MHTML file URIs to redirect the browser to a local resource. MHTML file URIs are used to specify the location of content embedded in an MHT file. MHTML URIs have the following format:

```
mhtml:[Mhtml_File_Uri]![Original_Resource_Uri]
```

It has been reported that if the resource specified in the Mhtml_File_Uri cannot be found, the browser will attempt to retrieve the resource specified in the Original_Resource_Uri. This works much like an HTTP redirect. Due to insufficient security checks when accessing the Original_Resource_Uri, it is possible to use this to redirect the browser to a local resource. This issue may be combined with BID 9105 in order to execute arbitrary code on a vulnerable system.

Symantec has confirmed that this issue is exploitable on IE 5.0 as well as the version tested by the researcher.

This issue was originally covered in BID 9100 "Multiple Internet Explorer Browser Security Model Compromise Vulnerabilities" and is now being assigned its own BID.

10. Microsoft Internet Explorer Window.MoveBy/Method Caching Mou...

BugTraq ID: 9108

Remote: Yes

Date Published: Nov 25 2003

Relevant URL: <http://www.securityfocus.com/bid/9108>

Summary:

Microsoft Internet Explorer is an Internet browser application that is shipped with Microsoft Windows. Internet Explorer provides support for JavaScript by default. window.moveBy(), is a JavaScript function that moves the current window on an x and y axis specified by arguments passed to the function. In BID 8755, it was reported that by using the window.moveBy() function an attacker could potentially hijack mouse click events and influence an Internet Explorer user into invoking unintended procedures. This vulnerability was addressed by the MS03-048 cumulative security update for Internet Explorer.

It has been reported that a variation on the attack described in BID 8755 has been discovered that will bypass security measures implemented in the MS03-048 cumulative security update. MS03-048 enforced measures to make the window.moveBy() function inaccessible, however it has been reported that by using JavaScript method caching functions(SaveRef) an attacker may again make the window.moveBy() function available and so may potentially hijack mouse click events.

An attacker may exploit this issue to hijack mouse click events and ultimately influence an unsuspecting user into invoking unintended procedures.

This issue was originally covered in BID 9100 "Multiple Internet Explorer Browser Security Model Compromise Vulnerabilities" and is now being assigned its own BID.

11. Microsoft Internet Explorer BackToFramedJPU Cross-Domain Pol...

BugTraq ID: 9109

Remote: Yes

Date Published: Nov 25 2003

Relevant URL: <http://www.securityfocus.com/bid/9109>

Summary:

A vulnerability has been reported in sub-frames in Microsoft Internet Explorer. Because of this, an attacker may be able to violate cross-domain policy.

The problem is a variation of vulnerabilities previously reported by Liu Die Yu (which are covered in BID 8577). The issue involves navigating sub-frames to a JavaScript protocol URI and the use of `history.back()`. The problem components could allow for script code to access properties of a page from a foreign domain, stored in the browser history. This issue, by itself, could permit a malicious web page to interact with a foreign domain, potentially allowing for theft of sensitive information or other attacks. By exploiting this issue in combination with other vulnerabilities (such as BIDs 9105 and 9107), it will be possible to execute malicious code on the client system in the context of the Local Zone.

Symantec has confirmed that this issue is exploitable on IE 5.0 as well as the version tested by the researcher.

Due to the ease of exploitation and the existence of other vulnerabilities which may be exploited in tandem with this BID, it is probable that this issue will be widely exploited in the wild.

This issue was originally covered in BID 9100 "Multiple Internet Explorer Browser Security Model Compromise Vulnerabilities" and is now being assigned its own BID.

12. Macromedia JRun Administrative Interface Multiple Cross-Site...

BugTraq ID: 9112

Remote: Yes

Date Published: Nov 26 2003

Relevant URL: <http://www.securityfocus.com/bid/9112>

Summary:

Macromedia JRun is a J2EE application server for use with IIS 4/5 on the Microsoft Windows operating systems.

Macromedia JRun includes a web-based administrative console which listens on TCP port 8000. When this page is accessed, the user is prompted for an administrative login.

It is said that an unauthenticated user may be capable of passing malicious script code embedded within URI parameters to the various scripts used by the interface, that will be interpreted by an authenticated user when the page is loaded.

This problem is said to occur due to the application failing to sanitize specific parameters passed to the `webserverlist.jsp`, `clusterframe.jsp`, `jrunwebserverconfig.jsp`, and `serverframe.jsp` script files.

An attacker could exploit this condition by constructing malicious links containing embedded script code and coaxing an administrative user to follow them. If followed, this could potentially allow an attacker to expose the administrators authentication credentials, ultimately allowing them to gain access to the interface. Access such as this could lead to further more serious attacks against specific hosts.

These issues are said to be present in Macromedia JRun 4 (build 61650) however, it is possible that other versions are also affected.

13. Microsoft Exchange Server 2003 Outlook Web Access Lowered Se...

BugTraq ID: 9118

Remote: No

Date Published: Nov 27 2003

Relevant URL: <http://www.securityfocus.com/bid/9118>

Summary:

Microsoft Exchange Server 2003 is an e-mail and directory server offered by Microsoft. Outlook Web Access (OWA) is a service provided by Exchange server that allows users to access their Exchange mailbox via the web.

A weakness is reported to exist in the software that may allow an attacker to gain unauthorized access to a user's mail through Outlook Web Access therefore gaining access to sensitive information.

The issue is reported to present itself when Microsoft Windows SharePoint Services 2.0 is installed on a machine running both Exchange Server 2003 and Microsoft Windows Server 2003. This installation may cause the Kerberos authentication employed by the server to be disabled in IIS (Internet Information Services) and OWA would fall back to the weaker NTLM authentication protocol. This may cause Exchange Server to incorrectly handle OWA requests as well. It has been reported that this issue may allow an attacker to gain unauthorized access to a user's mailbox that could result in a disclosure to sensitive information.

Due to a lack to details, exact attack information and exploitation cannot be specified at the moment. This BID will be updated as more information becomes available.

14. phpBB search.php SQL Injection Vulnerability

BugTraq ID: 9122

Remote: Yes

Date Published: Nov 27 2003

Relevant URL: <http://www.securityfocus.com/bid/9122>

Summary:

phpBB is an open-source web forum application that is written in PHP and supported by a number of database products. It will run on most Unix and Linux variants, as well as Microsoft Windows operating systems.

A vulnerability has been reported to exist in the software that may a remote user to inject malicious SQL syntax into database queries. The problem reportedly exists in the 'search_id' parameter of search.php

script. This issue is caused by insufficient sanitization of user-supplied data. A remote attacker may exploit this issue to influence SQL query logic to disclose sensitive information that could be used to gain unauthorized access.

A malicious user may influence database queries in order to view or modify sensitive information potentially compromising the software or the database.

phpBB version 2.06 has been prone to this issue, however other versions may be affected as well.

III. MICROSOFT FOCUS LIST SUMMARY

1. are my binaries being exposed on my ASP.NET website? (Thread)

Relevant URL:

<http://www.securityfocus.com/archive/88/345894>

2. local admin account password (Thread)

Relevant URL:

<http://www.securityfocus.com/archive/88/345893>

3. how do I force secure ASP.NET session cookies? (Thread)

Relevant URL:

<http://www.securityfocus.com/archive/88/345782>

4. Strange behaviour of MS SQL 2000 (Thread)

Relevant URL:

<http://www.securityfocus.com/archive/88/345550>

5. IIS traffic (Thread)

Relevant URL:

<http://www.securityfocus.com/archive/88/345549>

6. SecurityFocus Microsoft Newsletter #164 (Thread)

Relevant URL:

<http://www.securityfocus.com/archive/88/345505>

7. Administrivia: Article Announcements (Thread)

Relevant URL:

<http://www.securityfocus.com/archive/88/345503>

8. TS group policy / hide notification area (Thread)

Relevant URL:

<http://www.securityfocus.com/archive/88/345489>

9. Article Announcement: Busting the Worm Writers (Thread)

Relevant URL:

<http://www.securityfocus.com/archive/88/345487>

10. Betr.: Strange behaviour of MS SQL 2000 (Thread)

Relevant URL:

<http://www.securityfocus.com/archive/88/345444>

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. 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.

2. 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.

3. 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.

4. 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.

5. 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.

6. 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).

VI. SPONSOR INFORMATION

This Issue is Sponsored by: Tenable Security

Tenable provides security software which enables enterprises to distribute, manage, and communicate vulnerability and intrusion detection information across the entire organization. Tenable's breakthrough Lightning(tm) technology elegantly simplifies the complex nature of network security by offering detailed useable reports for network and security administrators and high-level organizational reports for CxOs. In addition, Tenable offers both active (NeWT) and passive (NeVO) vulnerability detection solutions to further enhance your network vulnerability identification. For more information, Tenable can be reached at 410-872-0555 or on the Internet at http://www.securityfocus.com/sponsor/TenableSecurity_ms-secnews_031201

