

SecurityFocus Microsoft Newsletter #50

Source: <http://www.derkeiler.com/Mailing-Lists/securityfocus/focus-ms/2001-09/0014.html>

From: Marc Fossi (mfossi@securityfocus.com)

Date: 09/04/01

Date: Tue, 4 Sep 2001 15:44:23 -0600 (MDT)
From: Marc Fossi <mfossi@securityfocus.com>
To: Focus-MS <focus-ms@securityfocus.com>
Subject: SecurityFocus Microsoft Newsletter #50
Message-ID: <Pine.GSO.4.30.0109041543430.2977-100000@mail>

SecurityFocus Microsoft Newsletter #50

This Issue Sponsored by: Foundstone

"Ultimate Hacking: Hands On – NT/2000 Security"

If you're running a Windows network, then this is the intensive 3-day course with everything a hacker knows...that you'll need to know! As a Specialist in Microsoft's Security Services Partner Program, Foundstone knows hacking, security and Microsoft. Register now for the class in New York City, September 25-27 and Irvine, CA December 11-13.

<http://www.foundstone.com/NT>

I. FRONT AND CENTER

1. ARIS Analyzer Version 1.5 Release
2. Introduction to Security Policies, Part One: An Overview of Policies
3. An Audit of Active Directory Security, Part Two: Understanding the Security Implications of Active Directory Default Settings
4. Network Monitoring for Intrusion Detection

II. MICROSOFT VULNERABILITY SUMMARY

1. Microsoft Windows 2000 IrDA Buffer Overflow Denial of Service...
2. Microsoft Outlook Web Access Denial of Service Vulnerability

III. MICROSOFT FOCUS LIST SUMMARY

1. A couple questions (Thread)
2. News question... (Thread)
3. Autopsy of a successful intrusion (well, two actually) (Thread)
4. Audit Tools (Thread)
5. Fluff was: RE: Audit Tools (Thread)
6. Network Trojan / Malware scanning tools (Thread)
7. Disabling a port on NT 4.0 Server (Thread)

8. Follow up on Trojan Scanner (Thread)
9. What I would like the MS IIS Lockdown tool todo (Thread)
10. Options for securing a Public Webserver and Private Intranet...
11. Options for securing a Public Webserver and Private Intranet...
12. Email webbugs (Thread)
13. Ms Proxy – concurrent access (Thread)
14. WIN2000 and IIS (Thread)
15. Help... (Thread)
16. Email webbugs (Eudora Rules) (Thread)
17. RE[2]: cmd.exe / root.exe question (Thread)
18. apache on NT (Thread)
19. cmd.exe / root.exe question (Thread)
20. SecurityFocus Microsoft Newsletter #49 (Thread)
21. Using IPSec as a Packet Filter Firewall (Thread)
22. MS IIS Lockdown tool (Thread)
23. Winpcap bindings (Thread)
24. IIS Help (Thread)
25. MPSA and password tests (Thread)
26. Proxy & Firewall for NT (Thread)
27. Transparent screensaver (Thread)

IV. NEW PRODUCTS FOR MICROSOFT PLATFORMS

1. Crypto Systems Toolkit
2. Sybergen Access Server
3. P-Synch Total Password Management Solution

V. NEW TOOLS FOR MICROSOFT PLATFORMS

1. DSNS network scanner v1.0
2. Chown
3. LinkLogger v1.2.0.279
4. Motorola Intrusion Vision (MIV)

VI. SPONSORSHIP INFORMATION

I. FRONT AND CENTER

1. ARIS Analyzer Version 1.5 Release

SecurityFocus is proud to announce the launch of ARIS analyzer version 1.5. Based on user feedback and lessons learned from the Code Red worm, we've greatly improved the system, its interface, and incident reporting capabilities.

For those who are not familiar with ARIS analyzer, it is a free service designed, administered and maintained by SecurityFocus to allow participating network administrators to submit suspicious network traffic and intrusion attempts anonymously, for detailed analysis and tracking. It allows the correlation and management of IDS data from a number of industry leading IDS' on a centralized incident management console.

It is available at the following URL:

<http://aris.securityfocus.com>

Here is a quick run-down of some of the new features that have been integrated into ARIS analyzer:

- A central message board that serves as a medium for the community to collaborate on important issues. New groups will be created for the discussion of specific incidents that arise, on an as-needed basis (CodeRed, Leaves, etc). This message board is separate from the incidents mailing list at SecurityFocus, and it specifically for ARIS Analyzer users.
- A second message board system used for hosting private discussions between ARIS Analyzer users who have a particular attacker in common.
- A vast number of enhancements on the Incidents screen that includes the ability to sort based upon a number of variables, the implementation of severity ratings, improved visibility of other affected ARIS users who have been attacked by the same IP, and much more.
- A complete overhaul of the ARIS analyzer reporting mechanism. A total of 32 reports can now be generated based upon uploaded incident data. This allows the ARIS analyzer to perform a quick tally on who is the top offending IP targeting their network, the most frequently attacked ports, the most commonly deployed attack types against the network, etc.
- Support for Symantec NetProwler has recently been added. Existing supported IDSs include Snort, NetworkICE BlackICE, ISS RealSecure, Dragon IDS, and Cisco Secure IDS with NFR NIDS to be integrated in the near future.

Down the road, we will continue to develop ARIS analyzer, improving it, and adding the features that the community is looking for. One feature currently in development is a customized home page that will display statistics and summary data that is specific to the user's network when logged in. As opposed to generating specific reports, this will give the user a high level overview of your infrastructure.

For those of you who are already registered as an ARIS analyzer user, we highly encourage you to take a look at the new site and send us your feedback at aris-feedback@securityfocus.com. Those who have not taken advantage of this free service yet can sign up at:

<http://aris.securityfocus.com>

Many users have asked how we are able to offer this service free of charge. ARIS Analyzer is a subset of a commercial service, ARIS Predictor, a predictive security intelligence service, backed by the SecurityFocus analyst team. This service uses global ARIS Analyzer data to provide customers with overviews and analysis' of events and trends. We will continue to develop ARIS Analyzer, in an effort to give you the features that you want in an incident management console. This approach is a balanced way to provide a powerful service free of charge to the community

and ensure that it is funded so that it might continue its existence.

Thanks for reading.

Oliver Friedrichs
Director of Engineering – ARIS
(650) 655-2000 X31

2. Introduction to Security Policies, Part One: An Overview of Policies by Charl van der Walt

This is the first in a series of four articles devoted to discussing about how information security policies can be used as an active part of an organization's efforts to protect its valuable information assets. In a world that is essentially technology driven; where the latest IIS exploit is countered with a mad rush to install the relevant patch and where the number of different operating systems in a network exceeds the number of hairs on the security administrator's head that haven't turned gray, policies give us an opportunity to change the pace, slow things down and play the game on our own terms.

<http://www.securityfocus.com/focus/basics/articles/policies.html>

3. An Audit of Active Directory Security, Part Two: Understanding the Security Implications of Active Directory Default Settings by Aaron Sullivan

In the last article, there was a brief introduction to Active Directory as it relates to LDAP, NT 4 directory services, and a few other things. Understanding the structural and syntactical layout of an LDAP/AD database was also covered in brief. Lastly, some general thoughts were given out about the implications of making a computer network as integrated, reliant, and controlled by a massive directory service like AD. In this article, we'll begin to approach AD security implications in a more technical manner.

<http://www.securityfocus.com/focus/microsoft/2k/adaudit2.html>

4. Network Monitoring for Intrusion Detection by Karen Frederick

In the world of intrusion detection, we tend to focus on detecting attacks and clearly anomalous activity. However, another important component of a complete intrusion detection solution is basic network monitoring and traffic analysis. Network monitoring collects information on connections, while traffic analysis allows us to see what services are being used on a network and to compare that against the activity that we should be seeing. This allows us to identify unauthorized services being used within a network, as well as gaps in network perimeter defenses.

<http://www.securityfocus.com/focus/ids/articles/networkmon.html>

II. BUGTRAQ SUMMARY

1. Microsoft Windows 2000 IrDA Buffer Overflow Denial of Service Vulnerability

BugTraq ID: 3215

Remote: Yes

Date Published: 2001-08-21

Relevant URL:

<http://www.securityfocus.com/bid/3215>

Summary:

IrDA (Infrared Data Association) is the standard protocol for transmitting data using infrared devices.

Microsoft Windows 2000's software which handles IrDA contains an unchecked buffer which could result in an overflow condition if sent a specifically crafted IrDA packet resulting in a system reboot. This vulnerability could result in a denial of service condition if the target system was continually sent these malformed packets.

IrDA devices are limited to line of sight range within approximately 3-4 feet.

There is currently no known way for this exploit to be used to run malicious code on the target system.

IrDA port communications are most commonly used by laptops.

2. Microsoft Outlook Web Access Denial of Service Vulnerability

BugTraq ID: 3223

Remote: Yes

Date Published: 2001-08-22

Relevant URL:

<http://www.securityfocus.com/bid/3223>

Summary:

Outlook Web Access is an optional component of Microsoft Exchange Server which runs in conjunction with Microsoft Internet Information Server. It provides access to a user's Exchange mailbox through a web interface.

A user can enter a long string of % characters into the Log On field in the Outlook Web Access logon page. Next, the NT challenge dialog will pop up requesting the username and password. The user enters the same long string into both the username and password fields and presses <enter> until the request times out.

At this point both the WWW Publishing service and the IIS Administration service are stopped. This results in the inability of the host server to fulfill HTTP requests or start the IIS Administration interface.

An administrator must manually restart the services to resume normal operation of the server.

Note: If this behaviour is due to a buffer overrun condition, it may be possible to execute arbitrary code on the server with administrative privileges.

III. MICROSOFT FOCUS LIST SUMMARY

1. A couple questions (Thread)

Relevant URL:

<http://www.securityfocus.com/frames/index.html?content=%2ftemplates%2farchive.pike%3flist%3d88%26date%3d20>

2. News question... (Thread)

Relevant URL:

<http://www.securityfocus.com/frames/index.html?content=%2ftemplates%2farchive.pike%3flist%3d88%26date%3d20>

3. Autopsy of a successful intrusion (well, two actually) (Thread)

Relevant URL:

<http://www.securityfocus.com/frames/index.html?content=%2ftemplates%2farchive.pike%3flist%3d88%26date%3d20>

4. Audit Tools (Thread)

Relevant URL:

<http://www.securityfocus.com/frames/index.html?content=%2ftemplates%2farchive.pike%3flist%3d88%26date%3d20>

5. Fluff was: RE: Audit Tools (Thread)

Relevant URL:

<http://www.securityfocus.com/frames/index.html?content=%2ftemplates%2farchive.pike%3flist%3d88%26date%3d20>

6. Network Trojan / Malware scanning tools (Thread)

Relevant URL:

<http://www.securityfocus.com/frames/index.html?content=%2ftemplates%2farchive.pike%3flist%3d88%26date%3d20>

7. Disabling a port on NT 4.0 Server (Thread)

Relevant URL:

<http://www.securityfocus.com/frames/index.html?content=%2ftemplates%2farchive.pike%3flist%3d88%26date%3d20>

8. Follow up on Trojan Scanner (Thread)

Relevant URL:

<http://www.securityfocus.com/frames/index.html?content=%2ftemplates%2farchive.pike%3flist%3d88%26date%3d20>

9. What I would like the MS IIS Lockdown tool todo (Thread)

Relevant URL:

af05a8c0@anchorsign.com"><http://www.securityfocus.com/frames/index.html?content=%2ftemplates%2farchive.pike>

SecurityFocus Microsoft: SecurityFocus Microsoft Newsletter #50

10. Options for securing a Public Webserver and Private Intranet on same server. (Thread)

Relevant URL:

<http://www.securityfocus.com/frames/index.html?content=%2ftemplates%2farchive.pike%3flist%3d88%26date%3d20>

11. Options for securing a Public Webserver and Private Intranet on same server. (Thread)

Relevant URL:

<http://www.securityfocus.com/frames/index.html?content=%2ftemplates%2farchive.pike%3flist%3d88%26date%3d20>

12. Email webbugs (Thread)

Relevant URL:

<http://www.securityfocus.com/frames/index.html?content=%2ftemplates%2farchive.pike%3flist%3d88%26date%3d20>

13. Ms Proxy – concurrent access (Thread)

Relevant URL:

<http://www.securityfocus.com/frames/index.html?content=%2ftemplates%2farchive.pike%3flist%3d88%26date%3d20>

14. WIN2000 and IIS (Thread)

Relevant URL:

<http://www.securityfocus.com/frames/index.html?content=%2ftemplates%2farchive.pike%3flist%3d88%26date%3d20>

15. Help... (Thread)

Relevant URL:

<http://www.securityfocus.com/frames/index.html?content=%2ftemplates%2farchive.pike%3flist%3d88%26date%3d20>

16. Email webbugs (Eudora Rules) (Thread)

Relevant URL:

<http://www.securityfocus.com/frames/index.html?content=%2ftemplates%2farchive.pike%3flist%3d88%26date%3d20>

17. RE[2]: cmd.exe / root.exe question (Thread)

Relevant URL:

<http://www.securityfocus.com/frames/index.html?content=%2ftemplates%2farchive.pike%3flist%3d88%26date%3d20>

18. apache on NT (Thread)

Relevant URL:

<http://www.securityfocus.com/frames/index.html?content=%2ftemplates%2farchive.pike%3flist%3d88%26date%3d20>

19. cmd.exe / root.exe question (Thread)

Relevant URL:

<http://www.securityfocus.com/frames/index.html?content=%2ftemplates%2farchive.pike%3flist%3d88%26date%3d20>

SecurityFocus Microsoft: SecurityFocus Microsoft Newsletter #50

20. SecurityFocus Microsoft Newsletter #49 (Thread)

Relevant URL:

<http://www.securityfocus.com/frames/index.html?content=%2ftemplates%2farchive.pike%3flist%3d88%26date%3d20>

21. Using IPSec as a Packet Filter Firewall (Thread)

Relevant URL:

<http://www.securityfocus.com/frames/index.html?content=%2ftemplates%2farchive.pike%3flist%3d88%26date%3d20>

22. MS IIS Lockdown tool (Thread)

Relevant URL:

[6501a8c0@ssr.hp.com">http://www.securityfocus.com/frames/index.html?content=%2ftemplates%2farchive.pike%3f](http://www.securityfocus.com/frames/index.html?content=%2ftemplates%2farchive.pike%3flist%3d88%26date%3d20)

23. Winpcap bindings (Thread)

Relevant URL:

<http://www.securityfocus.com/frames/index.html?content=%2ftemplates%2farchive.pike%3flist%3d88%26date%3d20>

24. IIS Help (Thread)

Relevant URL:

[d2e714d8@hack3r.org">http://www.securityfocus.com/frames/index.html?content=%2ftemplates%2farchive.pike%3f](http://www.securityfocus.com/frames/index.html?content=%2ftemplates%2farchive.pike%3flist%3d88%26date%3d20)

25. MPSA and password tests (Thread)

Relevant URL:

<http://www.securityfocus.com/frames/index.html?content=%2ftemplates%2farchive.pike%3flist%3d88%26date%3d20>

26. Proxy & Firewall for NT (Thread)

Relevant URL:

<http://www.securityfocus.com/frames/index.html?content=%2ftemplates%2farchive.pike%3flist%3d88%26date%3d20>

27. Transparent screensaver (Thread)

Relevant URL:

<http://www.securityfocus.com/frames/index.html?content=%2ftemplates%2farchive.pike%3flist%3d88%26date%3d20>

IV. NEW PRODUCTS FOR MICROSOFT PLATFORMS

1. Crypto Systems Toolkit

by Baltimore Technologies

Platforms: DOS, HP-UX, Linux, Solaris, Windows 3.x, Windows 95/98 and
Windows NT

Relevant URL:

<http://www.securityfocus.com/templates/product.html?id=580>

Summary:

CST contains implementations of the most popular and trusted cryptographic algorithms (RSA, DES, IDEA, etc.). These are accessed through BSAPI which enables developers to include cryptographic functions in their applications in a straightforward and consistent manner. In particular CST is applicable to all cryptographic techniques based on modular arithmetic. Such techniques include RSA, DSA, Fiat–Shamir, DL, Diffie–Hellman key exchange, etc.

2. Sybergen Access Server

by Sybergen Networks Inc.

Platforms: Linux, MacOS, UNIX, Windows 2000, Windows 95/98 and Windows NT

Relevant URL:

<http://www.securityfocus.com/templates/product.html?id=1296>

Summary:

Sybergen Access Server delivers Internet access management that provides shared Internet access, a secure firewall, and optimization to maximize the use of the available bandwidth. Sybergen Access Server turns any PC into an Internet gateway with enterprise–level management features, while protecting the computers on your network.

3. P–Synch Total Password Management Solution

by M–TECH

Platforms: AIX, DG–UX, HP–UX, IRIX, Linux, MVS, Netware, Solaris, SunOS, VMS and Windows NT

Relevant URL:

<http://www.securityfocus.com/templates/product.html?id=837>

Summary:

P–Synch is a total password management solution. It is intended to reduce the cost of ownership of password systems, and simultaneously improve the security of password protected systems. This is done through: –Password Synchronization. –Enforcing an enterprise wide password strength policy. –Allowing authenticated users to reset their own forgotten passwords and enable their locked out accounts. –Streamlining help desk call resolution for password resets. P–Synch is available for both internal use, on the corporate Intranet, as well as for the Internet deployment in B2B and B2C applications.

V. NEW TOOLS FOR MICROSOFT PLATFORMS

1. DSNS network scanner v1.0

by Hannes Gräuler

Relevant URL:

<http://www.securityfocus.com/tools/2183>

Platforms: Windows 2000

Summary:

DSNS is advanced network scanner for Windows 2000. It uses fast SYN scanning to find open ports and is able to probe the services that are running on that ports. So you can check proxys, scan for SMTP relaying

hosts and more.

2. Chown

by Richard Puckett, rpuckett@snl.com

Relevant URL:

<http://www.securityfocus.com/tools/1245>

Platforms: Windows NT

Summary:

CHOWN.ZIP is a GUI NT equivalent to the UNIX tool. Microsoft claims that the ownership process of NTFS file objects in NT is a two-part process, requiring that the user possess the right to take ownership (granted by the original object's owner/admin), then forcing them to execute the ownership right. This is to protect object ownership from "Rogue Administrators". This two-part ownership process is undesirable for administrators, who would prefer to just "give" ownership of file/directory objects to a particular user or group. This tool was written to show that the Owner ACL of a file/directory object can be overwritten with a modified replica Security Descriptor and elevated use of the SeRestorePrivilege (Tested to NT SP6). Source Code included with EXE.

3. LinkLogger v1.2.0.279

by Binary Visions Inc.

Relevant URL:

<http://www.securityfocus.com/tools/2089>

Platforms: Windows 95/98 and Windows NT

Summary:

Link Logger is a logging tool available for the Linksys BEF family of Routers. Link Logger lets you know what is happening at your router/firewall for both incoming and outgoing traffic. You will see who is knocking and what they are knocking with. Link Logger features alerts for suspicious traffic both coming into your network and leaving. You can even custom configure alarms to let you know the instant that traffic occurs to/from some IP address, or via some port.

4. Motorola Intrusion Vision (MIV)

by Motorola

Relevant URL:

<http://www.securityfocus.com/tools/2178>

Platforms: Windows 2000 and Windows NT

Summary:

Motorola Intrusion Vision (MIV) is a visualization and data management tool used with commercial and public domain intrusion detection systems. Alerts are analyzed in near-real time by the MIV Event Manager, graded by severity and categorized by type. The result is an intuitive graphical display leading to faster recognition of attacks and enabling a more timely response for better protection of your network.

VI. SPONSORSHIP INFORMATION

This Issue Sponsored by: Foundstone

"Ultimate Hacking: Hands On – NT/2000 Security"

If you're running a Windows network, then this is the intensive 3-day course with everything a hacker knows...that you'll need to know! As a Specialist in Microsoft's Security Services Partner Program, Foundstone knows hacking, security and Microsoft. Register now for the class in New York City, September 25–27 and Irvine, CA December 11–13.

<http://www.foundstone.com/NT>

- **Previous message:** [Oliver Friedrichs: "ARIS Analyzer Version 1.5"](#)
- **Messages sorted by:** [\[date \]](#) [\[thread \]](#) [\[subject \]](#) [\[author \]](#) [\[attachment \]](#)