

SecurityFocus Microsoft Newsletter #49

Source: <http://www.derkeiler.com/Mailing-Lists/securityfocus/focus-ms/2001-08/0496.html>

From: Marc Fossi (mfossi@securityfocus.com)

Date: 08/27/01

Date: Mon, 27 Aug 2001 12:39:36 -0600 (MDT)
From: Marc Fossi <mfossi@securityfocus.com>
To: Focus-MS <focus-ms@securityfocus.com>
Subject: SecurityFocus Microsoft Newsletter #49
Message-ID: <Pine.GSO.4.30.0108271238420.8037-100000@mail>

SecurityFocus Microsoft Newsletter #49

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. Keys to Successful Incident Response Teams
2. Introduction to Security Policies, Part One:
An Overview of Policies

II. MICROSOFT VULNERABILITY SUMMARY

1. Microsoft Windows NNTP Denial of Service Vulnerability
2. Microsoft IIS SSI Buffer Overrun Privelege Elevation Vulnerability
3. Microsoft IIS 4.0 URL Redirection DoS Vulnerability
4. Microsoft IIS 5.0 In-Process Table Privelege Elevation...
5. Microsoft IIS WebDAV Invalid Request Denial of Service...
6. Microsoft IIS MIME Header Denial of Service Vulnerability
7. Microsoft ISA Server H.323 Memory Leak Denial of Service...
8. Microsoft ISA Server Proxy Service Memory Leak Denial of...
9. Microsoft ISA Server Cross-Site Scripting Vulnerability
10. Microsoft Windows 2000 IrDA Buffer Overflow Denial of...

III. MICROSOFT FOCUS LIST SUMMARY

1. SV: Windows 2000's Everyone permission (Thread)
2. IRC zombies (Thread)

3. Windows 2000's Everyone permission (Thread)
 4. Some help understanding IIS / Site requirement.. (Thread)
 5. IIS 5 File Security (Thread)
 6. Proxy & Firewall for NT (Thread)
 7. MS IIS Lockdown tool (Thread)
 8. Win2K TCP/IP filtering and security (Thread)
 9. Directory Name (Thread)
 10. NT4 User List (Thread)
 11. Transparent screensaver (Thread)
 12. EFS and Biometrics? Other options? (Thread)
 13. Directory with name (Thread)
 14. removing front page extensions (Thread)
 15. FW: removing front page extensions (Thread)
 16. Remote Deletions (Thread)
 17. Tracking down a process under Windows NT/2000 (Thread)
 18. AW: RSA ACE Server on NT 4.0 (Thread)
 19. RSA ACE Server on NT 4.0 (Thread)
 20. MS patch-scanner for Win-NT, 2K, IIS, SQL (Thread)
 21. SP2 Stability Question... (Thread)
 22. strange file security properties (Thread)
 23. Using IPSEC to block IP (Thread)
 24. screensavers (Thread)
 25. Administrivia: FAQ (Thread)
 26. Introduction (Thread)
 27. Blocking a remote static IP in Windows 2000 (Thread)
 28. Beta Testers Needed, Part II (fwd) (Thread)
 29. SecurityFocus Microsoft Newsletter #48 (Thread)
 30. FW: Patched IIS/W2K Out of memory!!! (Thread)
 31. How to set user permissions? (Thread)
 32. MS01-044 (Thread)
 33. Kaspersky Labs has the answer? (Thread)
 34. virus or hack? (Thread)
 35. Infected with code red II ? (Thread)
 36. AW: Blocking a remote static IP in Windows 2000 (Thread)
 37. com2 (system devices) on IIS (Thread)
 38. problems with patch ms01-044 (Thread)
 39. Famatech Remote Administrator? (Thread)
 40. ACL for the mail root (Thread)
 41. Microsoft Knowledge Base Article – q305385 – Security Hotfix...
 42. Accessing mail from the web (Thread)
 43. Qchain.exe (Thread)
 44. Administrivia: A fond farewell (Thread)
 45. Accessing Exchange 2000 Remotely (Thread)
 46. MS01-044 & NT4 ... 2 files? (Thread)
 47. Disabling NetBIOS (Thread)
 48. Microsoft Security Bulletin MS01-044 (Thread)
 49. MPSA – Another security tool from MS (Thread)
 50. NTFS Access times (Thread)
 51. patch ms01-044 (Thread)
- IV. NEW PRODUCTS FOR MICROSOFT PLATFORMS
1. ZoneAlarm Pro 2.6

2. Solagent Secure
3. Lighthouse
4. VigilEnt Enterprise
5. SDK

V. NEW TOOLS FOR MICROSOFT PLATFORMS

1. wINJECT 0.95b
2. Bugnosis
3. Snort 1.8.1 Win32 Source
4. Passwords by Mask 1.42
5. Stunnel v3.20

VI. SPONSORSHIP INFORMATION

I. FRONT AND CENTER

1. Keys to Successful Incident Response Teams by Sarah Granger

In this article, the author talks about an increasing general awareness amongst organizations to become more tuned into security needs and developments. Building and deploying Incident Response Teams (IRTs) is the next logical step for organizations that have not yet done so, and so the writer walks you through the history, and the steps taken to form successful Incident Response Teams (IRTs), developing quality Incident Prevention and Educational policies, and forensic detail of computer crime.

<http://www.securityfocus.com/focus/ih/articles/successfulirt.html>

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 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. Policies allow organizations to set practices and procedures in place that will reduce the likelihood of an attack or an incident and will minimize the damage caused that such an incident can cause, should one occur.

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

II. BUGTRAQ SUMMARY

1. Microsoft Windows NNTP Denial of Service Vulnerability
BugTraq ID: 3183
Remote: Yes

Date Published: 2001-08-15

Relevant URL:

<http://www.securityfocus.com/bid/3183>

Summary:

Network News Transfer Protocol (NNTP) service is a protocol used to process posting, distributing, searching and archiving news articles posted to Usenet newsgroups. NNTP runs by default if Windows NT 4.0 Option Pack or Windows 2000 server is installed. It is not installed on default installations of Windows NT 4.0 and Windows 2000 Professional.

Due to a flaw in the Microsoft NNTP service, it is possible for a host to be led to consume all available memory resources. This behaviour is the result of flaws in the server's memory management.

Malformed news postings submitted repeatedly to an affected host, will result in the accumulation of allocated memory that is not freed after use. It is possible to exhaust the memory resources of the target system, potentially impacting the NNTP service and other applications running on the affected host.

A restart is required in order to gain normal functionality.

2. Microsoft IIS SSI Buffer Overrun Privelege Elevation Vulnerability

BugTraq ID: 3190

Remote: No

Date Published: 2001-08-15

Relevant URL:

<http://www.securityfocus.com/bid/3190>

Summary:

Microsoft Internet Information Server versions 4.0 and 5.0 use Server Side Includes (SSI). Server-Side Includes allow an author to include dynamic elements such as the current time on a website.

A user who has write permission to the web content folders of an IIS server can upload a malformed SSI command that, when executed would cause a buffer overrun resulting in any code of the user's choosing running in Local System context.

By default unprivileged users do not have the permission to upload content to an IIS server.

3. Microsoft IIS 4.0 URL Redirection DoS Vulnerability

BugTraq ID: 3191

Remote: Yes

Date Published: 2001-08-16

Relevant URL:

<http://www.securityfocus.com/bid/3191>

Summary:

A vulnerability exists in IIS 4.0 with URL redirection enabled, which could cause the server to stop responding.

The problem lies in IIS's handling of URL redirection. If a request is made which appears to be of accepted length, but in actuality the request reveals itself to be of unusual length IIS will fail.

This vulnerability is currently being exploited by the 'Code Red' worm. The worm sends a request to an IIS host attempting to exploit a previously discovered vulnerability (BID 2880). The request made contains incorrect length information which successfully affects normal functionality on a IIS 4.0 host.

A restart of the service is required in order to regain normal functionality.

4. Microsoft IIS 5.0 In-Process Table Privilege Elevation Vulnerability BugTraq ID: 3193

Remote: No

Date Published: 2001-08-15

Relevant URL:

<http://www.securityfocus.com/bid/3193>

Summary:

For performance reasons, Microsoft Internet Information Server 5.0 supports the ability to run certain executables 'in-process' when requested remotely.

When executables run 'in-process', they run as part of the main IIS process. It is important to restrict which executables can run 'in-process', because as part of the main IIS process they execute in the Local System security context.

IIS 5.0 ships with a table of executables that will run 'in-process' when requested by remote web clients. While all of these binaries are shipped with IIS, they are listed in the table using relative paths. A user who can create files on an IIS server can place an executable on the webroot filesystem with a relative path and filename that matches an entry in the table. When the executable is requested, its path and filename will cause it to be executed 'in-process'. The executable may provide administrative access for the attacker.

By default unprivileged users do not have the permission to upload content to an IIS server.

5. Microsoft IIS WebDAV Invalid Request Denial of Service Vulnerability BugTraq ID: 3194

Remote: Yes

Date Published: 2001-08-15

Relevant URL:

<http://www.securityfocus.com/bid/3194>

Summary:

WebDAV is an extension of the HTTP protocol and is installed by default with Microsoft IIS 5.0. WebDav enables remote users to manage and collaboratively edit files on remote web servers.

Microsoft IIS is subject to a denial of service attack. Because WebDAV contains a flaw in the handling of certain unusually long malformed requests, an attacker submitting such a request could cause the server to stop responding, leaving the server unable to accept any new HTTP sessions.

The duration of the denial of service is dependent on the actual length of the request. Once the malformed request comes to an end, the server will restart itself and regain normal functionality.

6. Microsoft IIS MIME Header Denial of Service Vulnerability

BugTraq ID: 3195

Remote: Yes

Date Published: 2001-08-15

Relevant URL:

<http://www.securityfocus.com/bid/3195>

Summary:

Due to Microsoft IIS's handling of MIME headers, a user could cause the server to stop responding.

The problem occurs when the server is preparing the MIME headers for the response to a HTTP request for a certain type of file. Under certain circumstances, a failure causing the server to stop responding may occur.

In order for this vulnerability to be successfully exploited, a user would need appropriate permissions to add content to the web server.

No further technical details are available at this time.

7. Microsoft ISA Server H.323 Memory Leak Denial of Service Vulnerability

BugTraq ID: 3196

Remote: Yes

Date Published: 2001-08-16

Relevant URL:

<http://www.securityfocus.com/bid/3196>

Summary:

The H.323 Gatekeeper Service in Microsoft ISA Server supports the transmission of voice-over-IP data through the firewall.

A certain type of malformed H.323 data can trigger a memory leak in the H.323 Gatekeeper Service. When the specially malformed data is received by the server, memory that is allocated is not freed. It is possible for an attacker to deplete memory by continuously sending this malformed data.

After enough malformed data is received, the ISA server could experience such a large degradation of performance that all traffic across the firewall would virtually cease.

Normal service could be restored by restarting the H.323 Gatekeeper Service.

8. Microsoft ISA Server Proxy Service Memory Leak Denial of Service Vulnerability

BugTraq ID: 3197

Remote: Yes

Date Published: 2001-08-16

Relevant URL:

<http://www.securityfocus.com/bid/3197>

Summary:

The Proxy Service in Microsoft ISA Server supports the sharing of HTTP access through the firewall.

A certain type of malformed data can trigger a memory leak in the Proxy Service. When the specially malformed data is received by the server, memory that is allocated is not freed. It is possible for an attacker to deplete memory by continuously sending this malformed data.

After enough malformed data is received, the ISA server could experience such a large degradation of performance that all traffic across the firewall would virtually cease.

It is important to note that this vulnerability is only available to users inside the network. Attackers from the Internet could not exploit this vulnerability.

Normal service could be restored by restarting the Proxy Service.

9. Microsoft ISA Server Cross-Site Scripting Vulnerability

BugTraq ID: 3198

Remote: Yes

Date Published: 2001-08-16

Relevant URL:

<http://www.securityfocus.com/bid/3198>

Summary:

Microsoft Internet Security and Acceleration (ISA) Server is a configurable firewall and proxy server. ISA Server implements secure internet access and accelerates internet usage through caching. The Web Proxy service (W3PROXY.EXE) enables internal users to make requests for external web resources via the firewall. This ensures that internal user requests are fulfilled through secure transactions.

Microsoft ISA Server does not protect against cross-site scripting attacks.

When ISA cannot retrieve a web document, it returns an error webpage containing the URL that was requested. It is possible for attackers to construct urls that will cause scripting code to be embedded in the error page.

Microsoft ISA Server fails to check the URL for the presence of script commands when generating the error page, allowing the attacker-supplied code to execute as content originating from the server returning the error message (even though the script commands may have originated at another site entirely).

This poses a serious security threat if the server specified in the requested URL is a trusted site, as content from that site may be granted a higher privilege level.

Successful exploitation of this vulnerability could enable an attacker to execute code in the security context of a trusted site. In addition, this issue could allow an attacker to access the trusted site's cookies, possibly aiding in other web-based attacks.

10. 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.

III. MICROSOFT FOCUS LIST SUMMARY

1. SV: Windows 2000's Everyone permission (Thread)

Relevant URL:

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

2. IRC zombies (Thread)

Relevant URL:

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

3. Windows 2000's Everyone permission (Thread)

Relevant URL:

[0b00010a@lauradominion.com">http://www.securityfocus.com/frames/index.html?content=%2ftemplates%2farchive.pike%3flist%3d88%26date%3d20](http://www.securityfocus.com/frames/index.html?content=%2ftemplates%2farchive.pike%3flist%3d88%26date%3d20)

4. Some help understanding IIS / Site requirement.. (Thread)

Relevant URL:

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

5. IIS 5 File Security (Thread)

Relevant URL:

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

6. Proxy & Firewall for NT (Thread)

Relevant URL:

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

7. MS IIS Lockdown tool (Thread)

Relevant URL:

[6c01a8c0@USWEST.NET">http://www.securityfocus.com/frames/index.html?content=%2ftemplates%2farchive.pike%3flist%3d88%26date%3d20](http://www.securityfocus.com/frames/index.html?content=%2ftemplates%2farchive.pike%3flist%3d88%26date%3d20)

8. Win2K TCP/IP filtering and security (Thread)

Relevant URL:

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

9. Directory Name (Thread)

Relevant URL:

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

10. NT4 User List (Thread)

Relevant URL:

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

11. Transparent screensaver (Thread)

Relevant URL:

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

12. EFS and Biometrics? Other options? (Thread)

Relevant URL:

[0b00010a@lauradominion.com">http://www.securityfocus.com/frames/index.html?content=%2ftemplates%2farchive.pike%3flist%3d88%26date%3d20](http://www.securityfocus.com/frames/index.html?content=%2ftemplates%2farchive.pike%3flist%3d88%26date%3d2000010a@lauradominion.com)

13. Directory with name (Thread)

Relevant URL:

[http://www.securityfocus.com/frames/index.html?content=%2ftemplates%2farchive.pike%3flist%3d88%26date%3d20](http://www.securityfocus.com/frames/index.html?content=%2ftemplates%2farchive.pike%3flist%3d88%26date%3d2000010a@lauradominion.com)

14. removing front page extensions (Thread)

Relevant URL:

[http://www.securityfocus.com/frames/index.html?content=%2ftemplates%2farchive.pike%3flist%3d88%26date%3d20](http://www.securityfocus.com/frames/index.html?content=%2ftemplates%2farchive.pike%3flist%3d88%26date%3d2000010a@lauradominion.com)

15. FW: removing front page extensions (Thread)

Relevant URL:

[http://www.securityfocus.com/frames/index.html?content=%2ftemplates%2farchive.pike%3flist%3d88%26date%3d20](http://www.securityfocus.com/frames/index.html?content=%2ftemplates%2farchive.pike%3flist%3d88%26date%3d2000010a@lauradominion.com)

16. Remote Deletions (Thread)

Relevant URL:

[http://www.securityfocus.com/frames/index.html?content=%2ftemplates%2farchive.pike%3flist%3d88%26date%3d20](http://www.securityfocus.com/frames/index.html?content=%2ftemplates%2farchive.pike%3flist%3d88%26date%3d2000010a@lauradominion.com)

17. Tracking down a process under Windows NT/2000 (Thread)

Relevant URL:

[http://www.securityfocus.com/frames/index.html?content=%2ftemplates%2farchive.pike%3flist%3d88%26date%3d20](http://www.securityfocus.com/frames/index.html?content=%2ftemplates%2farchive.pike%3flist%3d88%26date%3d2000010a@lauradominion.com)

18. AW: RSA ACE Server on NT 4.0 (Thread)

Relevant URL:

[http://www.securityfocus.com/frames/index.html?content=%2ftemplates%2farchive.pike%3flist%3d88%26date%3d20](http://www.securityfocus.com/frames/index.html?content=%2ftemplates%2farchive.pike%3flist%3d88%26date%3d2000010a@lauradominion.com)

19. RSA ACE Server on NT 4.0 (Thread)

Relevant URL:

[http://www.securityfocus.com/frames/index.html?content=%2ftemplates%2farchive.pike%3flist%3d88%26date%3d20](http://www.securityfocus.com/frames/index.html?content=%2ftemplates%2farchive.pike%3flist%3d88%26date%3d2000010a@lauradominion.com)

20. MS patch-scanner for Win-NT, 2K, IIS, SQL (Thread)

Relevant URL:

[http://www.securityfocus.com/frames/index.html?content=%2ftemplates%2farchive.pike%3flist%3d88%26date%3d20](http://www.securityfocus.com/frames/index.html?content=%2ftemplates%2farchive.pike%3flist%3d88%26date%3d2000010a@lauradominion.com)

21. SP2 Stability Question... (Thread)

Relevant URL:

[b403a8c0@AnchorSign.com">http://www.securityfocus.com/frames/index.html?content=%2ftemplates%2farchive.pike%3flist%3d88%26date%3d20](http://www.securityfocus.com/frames/index.html?content=%2ftemplates%2farchive.pike%3flist%3d88%26date%3d2000010a@lauradominion.com)

22. strange file security properties (Thread)

Relevant URL:

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

23. Using IPSEC to block IP (Thread)

Relevant URL:

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

24. screensavers (Thread)

Relevant URL:

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

25. Administrivia: FAQ (Thread)

Relevant URL:

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

26. Introduction (Thread)

Relevant URL:

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

27. Blocking a remote static IP in Windows 2000 (Thread)

Relevant URL:

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

28. Beta Testers Needed, Part II (fwd) (Thread)

Relevant URL:

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

29. SecurityFocus Microsoft Newsletter #48 (Thread)

Relevant URL:

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

30. FW: Patched IIS/W2K Out of memory!!! (Thread)

Relevant URL:

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

31. How to set user permissions? (Thread)

Relevant URL:

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

32. MS01-044 (Thread)

Relevant URL:

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

33. Kaspersky Labs has the answer? (Thread)

Relevant URL:

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

34. virus or hack? (Thread)

Relevant URL:

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

35. Infected with code red II ? (Thread)

Relevant URL:

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

36. AW: Blocking a remote static IP in Windows 2000 (Thread)

Relevant URL:

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

37. com2 (system devices) on IIS (Thread)

Relevant URL:

[13d0cbc7@Netvision.net.il">http://www.securityfocus.com/frames/index.html?content=%2ftemplates%2farchive.pike](http://www.securityfocus.com/frames/index.html?content=%2ftemplates%2farchive.pike%3flist%3d88%26date%3d20)

38. problems with patch ms01-044 (Thread)

Relevant URL:

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

39. Famatech Remote Administrator? (Thread)

Relevant URL:

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

40. ACL for the mail root (Thread)

Relevant URL:

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

41. Microsoft Knowledge Base Article – q305385 – Security Hotfix Checker tool (Thread)

Relevant URL:

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

42. Accessing mail from the web (Thread)

Relevant URL:

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

43. Qchain.exe (Thread)

Relevant URL:

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

44. Administrivia: A fond farewell (Thread)

Relevant URL:

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

45. Accessing Exchange 2000 Remotely (Thread)

Relevant URL:

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

46. MS01-044 & NT4 ... 2 files? (Thread)

Relevant URL:

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

47. Disabling NetBIOS (Thread)

Relevant URL:

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

48. Microsoft Security Bulletin MS01-044 (Thread)

Relevant URL:

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

49. MPSA – Another security tool from MS (Thread)

Relevant URL:

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

50. NTFS Access times (Thread)

Relevant URL:

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

51. patch ms01-044 (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. ZoneAlarm Pro 2.6

by Zone Labs

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

Relevant URL:

<http://www.securityfocus.com/templates/product.html?id=1338>

Summary:

ZoneAlarm Pro provides one-click support for small and home office networks, making it quick and easy to provide optimal security for all PCs on your network. Businesses can easily custom-fit ZoneAlarm Pro to their security needs to protect all Internet- or network-connected PCs by using default, company-wide settings or by using ZoneAlarm Pro's expert network administrator tools.

2. Solagent Secure

by Solagent

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

Relevant URL:

<http://www.securityfocus.com/templates/product.html?id=1421>

Summary:

This is our most cost effective monitoring service designed to provide you with the peace of mind that if your data is lost or stolen it still can be protected, remotely. Once you have discovered that your portable device is missing you are able to protect your data by contacting our Data Protection Center* either by logging on to our subscriber web site or by calling our toll free subscriber number. The Basic service gives you two choices: you may either encrypt your data or you may delete your data. Either option will help prevent others from using the data. The easy to use procedures are designed to make protection of your data simple. Ordering, registration and download is a snap, typically taking only a couple of minutes. During registration you can select the data you want protected in the event your device becomes lost or stolen. The basic service is \$29.95 for one year or \$49.95 for two years.

3. Lighthouse

by Waveset Technologies

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

Relevant URL:

<http://www.securityfocus.com/templates/product.html?id=1490>

Summary:

Waveset Lighthouse provides integrated functionality that spans identity management, user self-service, web single sign-on Management and active risk analysis with one purchase, one implementation and one product to support and maintain.

4. VigilEnt Enterprise

by PentaSafe

Platforms: AS/400, UNIX and Windows NT

Relevant URL:

<http://www.securityfocus.com/templates/product.html?id=1166>

Summary:

VigilEnt Enterprise is host-based security auditing/vulnerability assessment software for Windows NT, UNIX, IBM AS/400 systems and various applications, such as Web Servers. VigilEnt Enterprise is unique because it allows the administrator to pinpoint and check for a key security vulnerability issue across an enterprise in one report across multiple systems and regardless of platform. The administrator can then take action to repair the vulnerability across multiple systems directly from the VigilEnt Enterprise on-screen report. Furthermore, VigilEnt Enterprise provides the most detailed information about platform specific security issues as well all from one central console.

5. SDK

by Ankari Inc.

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

Relevant URL:

<http://www.securityfocus.com/templates/product.html?id=1488>

Summary:

Ankari provides complete support to third-party developers through its multi-platform Software Development Kit (SDK).

Custom applications with full biometric or biometric and smart card authentication capabilities can be developed quickly and easily with the SDK. Turnkey user interface components mean no understanding of biometrics is necessary, allowing the developer to focus on the application requirements rather than secure authentication.

The SDK's C-language Application Programming Interface (API) lets you develop in C, C++ or any environment able to call C functions (Visual Basic or Delphi, for example).

V.NEW TOOLS FOR MICROSOFT PLATFORMS

1. wINJECT 0.95b

by moofz

Relevant URL:

<http://www.securityfocus.com/tools/1893>

Platforms: Windows 95/98

Summary:

Winject is a low-level packet builder/injector for win9x dialup users. It allows you to create custom packets with real or spoofed IP addresses.

2. Bugnosis

by Privacy Foundation.

Relevant URL:

<http://www.securityfocus.com/tools/2172>

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

Summary:

Bugnosis is a Web bug detector. As you surf the Web, it analyzes every page you visit and alerts you when it finds any Web bugs. With Bugnosis, you don't have to be a code expert to tell when your browsing habits are being observed.

3. Snort 1.8.1 Win32 Source

by Michael Davis

Relevant URL:

<http://www.securityfocus.com/tools/1581>

Platforms: Windows 95/98 and Windows NT

Summary:

Snort is a lightweight network intrusion detection system, capable of performing real-time traffic analysis and packet logging on IP networks. It can perform protocol analysis, content searching/matching and can be used to detect a variety of attacks and probes, such as buffer overflows, stealth port scans, CGI attacks, SMB probes, OS fingerprinting attempts, and much more. Snort uses a flexible rules language to describe traffic that it should collect or pass, as well as a detection engine that utilizes a modular plugin architecture. Snort has a real-time alerting capability as well, incorporating alerting mechanisms for syslog, a user specified file, a UNIX socket, or WinPopup messages to Windows clients using Samba's smbclient.

4. Passwords by Mask 1.42

by Segobit Software

Relevant URL:

<http://www.securityfocus.com/tools/1957>

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

Summary:

Passwords by Mask is a application designed to generate passwords of any character content. It allow users to choose the type of password symbols. You can to fix random or specified alphabetic, random or specified numeric, random or specified alphanumeric, random or specified special or random or specified all keyboard characters for every password symbol. This feature allows users to generate a User ID and Password at random and at the same time. Passwords by Mask can to use Windows clipboard for transferring passwords between the program and other applications. All passwords can be printed.

5. Stunnel v3.20

by Michal Trojnara

Relevant URL:

<http://www.securityfocus.com/tools/988>

Platforms: FreeBSD, Linux, Windows 2000, Windows 95/98 and Windows NT

Summary:

The stunnel program is designed to work as an SSL encryption wrapper between remote client and local (inetd-startable) or remote server. It can be used to add SSL functionality to commonly used inetd daemons like POP2, POP3, and IMAP servers without any changes in the programs' code. It will negotiate an SSL connection using the OpenSSL or SSLeay libraries. It calls the underlying crypto libraries, so stunnel supports whatever cryptographic algorithms you compiled into your crypto package. This release includes a timeout for the transfer() function, and a fix for a coredump on exit with active threads.

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:** edgar.mendez@delphiauto.com: "Re: Email webbugs"
- **Messages sorted by:** [\[date \]](#) [\[thread \]](#) [\[subject \]](#) [\[author \]](#) [\[attachment \]](#)