

encryption security scan report

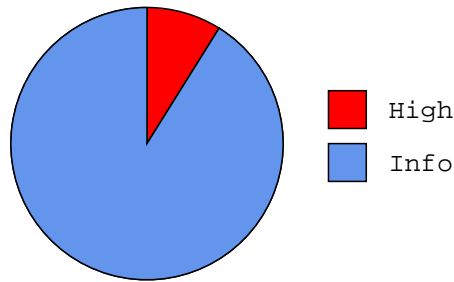
Scan time: 19/02/2007 14:00:00

Profile: PRODUCTION - SCAN

Total number of vulnerabilities identified on 1 system(s)

High : 1

Info : 10



Total number of vulnerabilities identified per system

Host	Serious	High	Medium	Medium/Low	Low/Medium	Low	Info
81.179.97.94	--	1	--	--	--	--	10

Host	Service	Risk	Description
81.179.97.94	ftp (21/tcp)	High	<p>FTP (File Transfer Protocol)</p> <p>FTP is the protocol used on the Internet for exchanging files.</p> <p>FTP is most commonly used to download a file from a server using the Internet or to upload a file to a server (eg, uploading a Web page file to a server. This family of tests checks whether a server could be putting sensitive data at risk by running insecure or outdated FTP services.</p> <p>Please read the technical information below for further information on this vulnerability.</p> <p>It might be possible to make the remote FTP server crash by issuing this command :</p> <p>CEL aaaa(...)aaaa</p> <p>This problem is similar to the <code>&#039;aix ftpd&#039;</code> overflow but on embedded vxworks based systems like the 3com nbx IP phone call manager and seems to cause the server to crash.</p> <p>*** Note that Nessus solely relied on the banner of *** the remote server to issue this warning.</p> <p>Solution: If you are using an embedded vxworks product, please contact the OEM vendor and reference WindRiver field patch TSR 296292. If this is the 3com NBX IP Phone call manager, contact 3com.</p> <p>This affects VxWorks ftpd versions 5.4 and 5.4.2</p>

			<p>For more information, see CERT VU 317417 http://www.kb.cert.org/vuls/id/317417 or full security alert at http://www.secnap.net/security/nbx001.html</p> <p>BID : 6297 Other references : OSVDB:17618</p>
81.179.97.94	ftp (21/tcp)	Info	
81.179.97.94	ftp (21/tcp)	Info	<p>Service detection</p> <p>Service detection protocols allow automatic detection of devices and services on a computer network. If a server is open to attacks on these protocols, then the server is vulnerable to, amongst others, a Denial of Service Attack. This family of tests checks whether a server is vulnerable to DoS attacks.</p> <p>Please read the technical information below for further details on this vulnerability.</p> <p>An FTP server is running on this port. Here is its banner : 220 VxWorks (5.4.1) FTP server ready</p>
81.179.97.94	ftp (21/tcp)	Info	<p>Service detection</p> <p>Service detection protocols allow automatic detection of devices and services on a computer network. If a server is open to attacks on these protocols, then the server is vulnerable to, amongst others, a Denial of Service Attack. This family of tests checks whether a server is vulnerable to DoS attacks.</p> <p>Please read the technical information below for further details on this vulnerability.</p> <p>Synopsis :</p> <p>An FTP server is listening on this port</p> <p>Description :</p> <p>It is possible to obtain the banner of the remote FTP server by connecting to the remote port.</p> <p>Plugin output :</p> <p>The remote FTP banner is : 220 VxWorks (5.4.1) FTP server ready</p>
81.179.97.94	general/icmp	Info	<p>Firewalls</p> <p>A firewall is a piece of hardware and/or software which aims to control communications into and out of a networked environment such as an office.</p> <p>Firewalls have to leave certain ports open for the operation of web, mail, ftp and other Internet based services - leaving you vulnerable to exploitation.</p> <p>Synopsis :</p>

			<p>It is possible to determine the exact time set on the remote host.</p> <p>Description :</p> <p>The remote host answers to an ICMP timestamp request. This allows an attacker to know the date which is set on your machine.</p> <p>This may help him to defeat all your time based authentication protocols.</p> <p>Solution : filter out the ICMP timestamp requests (13), and the outgoing ICMP timestamp replies (14).</p> <p>CVSS Base Score : 0 (AV:R/AC:L/Au:NR/C:N/A:N/I:N/B:N)</p> <p>Plugin output :</p> <p>The difference between the local and remote clocks is 50169 seconds</p> <p>CVE : CVE-1999-0524</p>
81.179.97.94	general/tcp	Info	<p>Misc.</p> <p>This is a miscellaneous family of security checks that do not fall clearly into any other family. Please read the technical information below for further details.</p> <p>The following ports were open at the beginning of the scan but are now closed:</p> <p>Port 80 was detected as being open but is now closed.</p> <p>This might be an availability problem related which might be due to the following reasons :</p> <ul style="list-style-type: none"> - The remote host is now down, either because a user turned it off during the scan - A network outage has been experienced during the scan, and the remote network cannot be reached from the Vulnerability Scanner any more - This Vulnerability Scanner has been blacklisted by the system administrator or by automatic intrusion detection/prevention systems which have detected the vulnerability assessment. <p>In any case, the audit of the remote host might be incomplete and may need to be done again</p>
81.179.97.94	general/tcp	Info	<p>General</p> <p>This family of tests checks for a variety of general security issues. Please read the technical information below for further information.</p> <p>The remote host is running HP JetDirect</p>
81.179.97.94	http (80/tcp)	Info	
81.179.97.94	http (80/tcp)	Info	<p>Service detection</p> <p>Service detection protocols allow automatic detection of devices and services on a computer network. If a server is open to attacks on these protocols, then the server is vulnerable to, amongst others, a Denial of Service Attack. This family of tests checks</p>

whether a server is vulnerable to DoS attacks.

Please read the technical information below for further details on this vulnerability.

A web server is running on this port

81.179.97.94	http (80/tcp)	Info	<p>Web Servers</p> <p>The term Web server can mean one of two things:</p> <p>A computer that is responsible for accepting requests from web browsers, and serving them Web pages or a computer program that provides the functionality described in the first sense of the term.</p> <p>The two most widely used web servers are Microsoft IIS and the open source 'Apache' web server. This family of tests identifies which web server(s) is/are running on a machine and runs a series of tests to determine whether they are vulnerable to attack.</p> <p>For further information on this vulnerability please read the technical description below.</p> <p>Synopsis :</p> <p>Some information about the remote HTTP configuration can be extracted.</p> <p>Description :</p> <p>This test gives some information about the remote HTTP protocol - the version used, whether HTTP Keep-Alive and HTTP pipelining are enabled, etc...</p> <p>This test is informational only and does not denote any security problem</p> <p>Solution :</p> <p>None.</p> <p>CVSS Base Score : 0 (AV:R/AC:L/Au:NR/C:N/A:N/I:N/B:N)</p> <p>Plugin output :</p> <p>Protocol version : HTTP/1.0 SSL : no Pipelining : no Keep-Alive : no Options allowed : (Not implemented) Headers :</p> <p>Connection: close Server: WindWeb/1.0.2 Date: TUE JAN 06 20:58:16 1970 Content-Type: text/html WWW-Authenticate: Basic realm="Home Gateway"</p>
--------------	---------------	------	----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

81.179.97.94	http (80/tcp)	Info	<p>General</p> <p>This family of tests checks for a variety of general security issues. Please read the technical information below for further information.</p> <p>The remote web server type is :</p> <p>WindWeb/1.0.2</p>
--------------	---------------	------	------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

encription security scan results