

PCI Detailed report

For

O24 PCI TEST



Sections -

- >> [Report info](#)
- >> [PCI - Overall status](#)
- >> [PCI - Host status](#)
- >> [Executive summary - Security Risk Overview](#)
- >> [Executive summary - Security Threat Families](#)
- >> [Host list summary](#)
- >> [Executive summary - Security Top Port List](#)
- >> [Open port list](#)
- >> [Vulnerability details](#)



Report info -

Report type:	PCI Detailed report
Report id:	5B75B7598FD1622DEF9465C6A026F3BD
Report Creation Date:	2008-03-14 14:05, GMT
Report creator:	pcitest for O24 PCI TEST
Schedule job:	103.2
Report Interval:	Latest: 2007-12-15 23:59 - 2008-03-14 23:59
Number of tests:	1
Number of threats/infos found:	37
	<p>This report was generated by a PCI Approved Scanning Vendor, Outpost24 AB, under certificate number 4047-01-01 within the guidelines of the PCI data security initiative.</p>




PCI Overall status -

PCI Status

Number of IPs scanned: 1 FAILED

Outpost24 has determined that
pcitest is NOT COMPLIANT with the
PCI scan validation requirement.

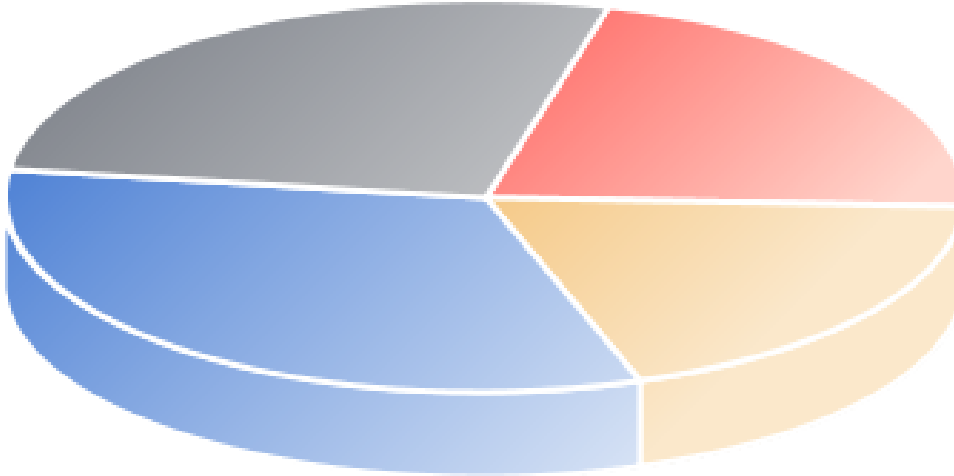
 **PCI Host status -**

PCI Status

192.168.103.2

FAILED

Executive summary - Security Risk Overview -



● Critical/Urgent = 8 ● High = 7 ● Medium = 12 ● Low = 10

[Critical/Urgent]

These vulnerabilities provide remote intruders with/without remote root or remote administrator capabilities. With this level of vulnerability, hackers can compromise the entire host. The vulnerabilities that provide remote hackers full file-system read and write capabilities or partial access to file-systems (for example, full read access without full write access), remote execution of commands as a root or administrator user. Vulnerabilities that expose highly sensitive information also qualify as these vulnerabilities. The presence of back doors and Trojan horses also qualify as these vulnerabilities. Severity level 4/5. Vulnerabilities with CVSS ratings 8.0-10.0 are also considered Critical/Urgent.

[High]

These vulnerabilities provide hackers with access to specific information stored on the host, including security settings. This level of vulnerabilities could result in potential misuse of the host by intruders. Examples of vulnerabilities include partial disclosure of file contents, access to certain files on the host, directory browsing, disclosure of filtering rules and security mechanisms, susceptibility to denial of service (DoS) attacks, and unauthorized use of services (for example, mail relaying). Severity level 3. Vulnerabilities with CVSS ratings 6.0-7.9 are also considered High.

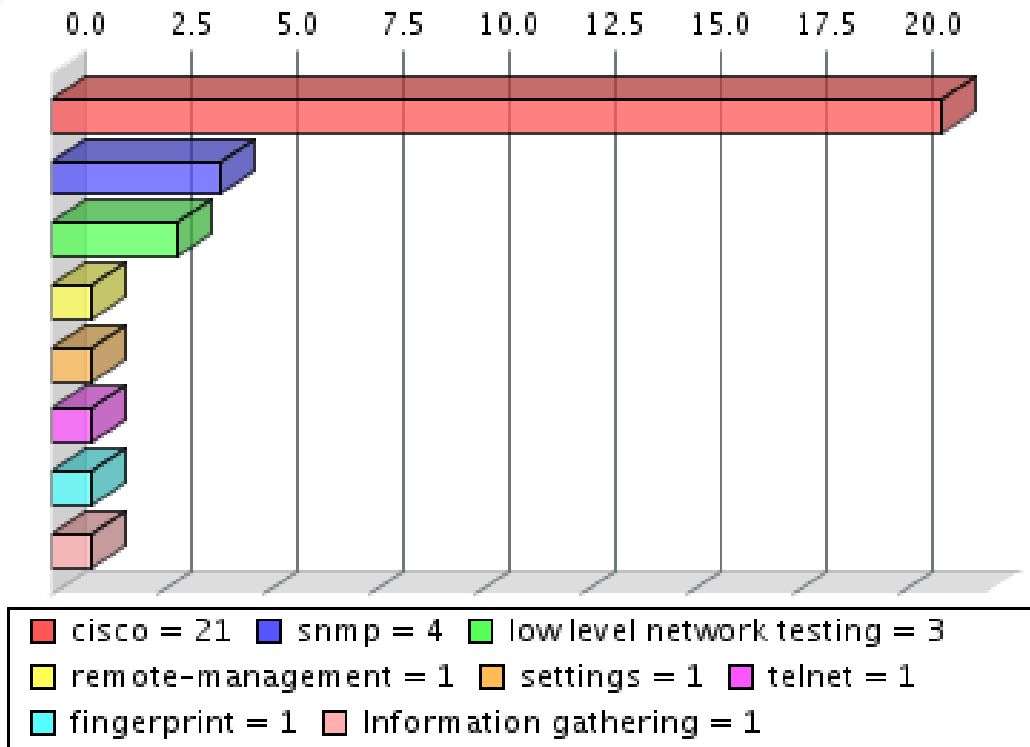
[Medium]

These vulnerabilities expose some sensitive information from the host, such as precise versions of services. With this information, hackers could research potential attacks to try against a host. Severity level 2. Vulnerabilities with CVSS ratings 4.0-5.9 are also considered Medium.

[Low]

These vulnerabilities are information such as open ports. Severity level 1. Vulnerabilities with CVSS ratings 0-3.9 are also considered Low.

Executive summary - Security Threat Families -



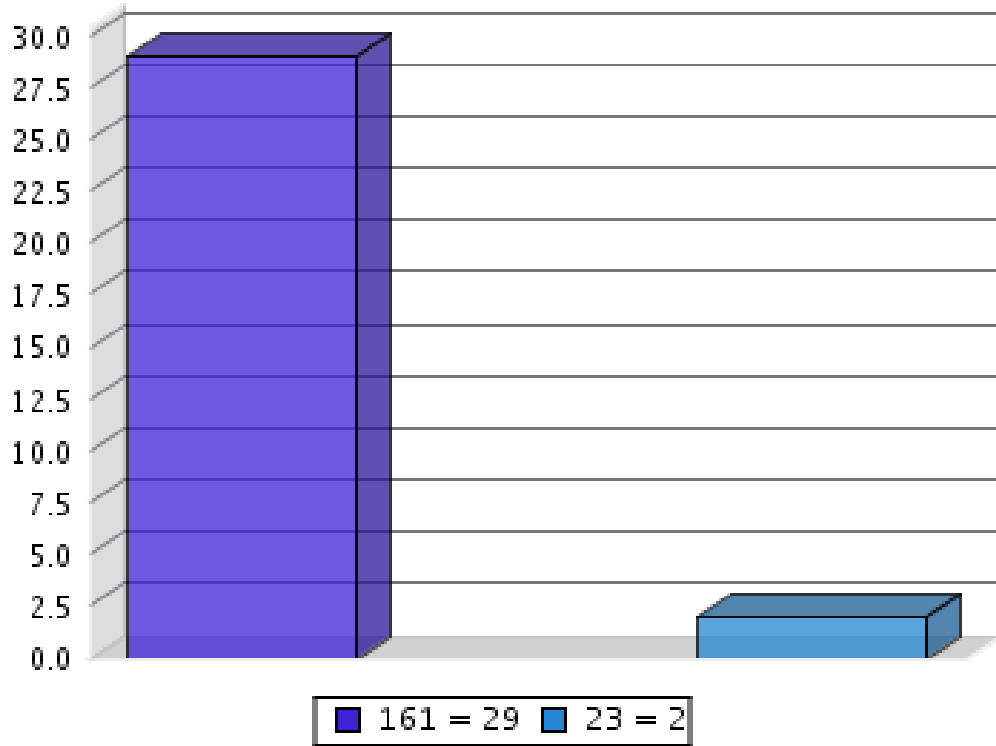
Family List:

This part of the report list the families with threats detected.

Host list summary -

	Critical/Urgent	High	Medium	Low	Open ports
192.168.103.2	8	7	12	10	2
Start: 2008-03-13 16:02		Template: None			
End: 2008-03-13 16:08					

Executive summary - Security Top Port List -



[Top Port]

This part of the report list the ports with highest number of threats.

Open port list -

192.168.103.2 23/tcp - telnet
2008-03-13 16:02 161/udp - snmp

 Vulnerability details - 192.168.103.2

Check id:	1040037
Name:	Cisco IOS Vulnerability
Port:	161/udp - snmp
Risk factor:	Critical/Urgent
CVSS	10.0 (AV:N/AC:L/Au:N/C:C/I:C/A:C)
Family:	cisco
Description:	Cisco IOS 9.x, 10.x, 11.x, and 12.x and IOS XR 2.0.x, 3.0.x, and 3.2.x allows remote attackers to cause a denial of service or execute arbitrary code via a crafted IP option in the IP header in a (1) ICMP, (2) PIMv2, (3) PGM, or (4) URD packet.
Solution:	Upgrade to a version of Cisco IOS that includes a fix to this problem
Reference:	url - http://www.cisco.com
CVE:	CVE-2007-0480
IPs:	192.168.103.2 - 2008-03-13 16:02

Check id:	1040097
Name:	Cisco IOS Vulnerability
Port:	161/udp - snmp
Risk factor:	Critical/Urgent
CVSS	10.0 (AV:N/AC:L/Au:N/C:C/I:C/A:C)
Family:	cisco
Description:	Cisco IOS 12.2(15) and earlier allows remote attackers to cause a denial of service (refused VTY (virtual terminal) connections), via a crafted TCP connection to the Telnet or reverse Telnet port.
Solution:	Upgrade to a version of Cisco IOS that includes a fix to this problem
Reference:	url - http://www.cisco.com
CVE:	CVE-2004-1464
IPs:	192.168.103.2 - 2008-03-13 16:02

Check id:	1040097
Name:	Cisco IOS Vulnerability
Port:	161/udp - snmp
Risk factor:	Critical/Urgent
CVSS	10.0 (AV:N/AC:L/Au:N/C:C/I:C/A:C)
Family:	cisco
Description:	Cisco IOS 12.2(15) and earlier allows remote attackers to cause a denial of service (refused VTY (virtual terminal) connections), via a crafted TCP connection to the Telnet or reverse Telnet port.
Solution:	Upgrade to a version of Cisco IOS that includes a fix to this problem
Reference:	url - http://www.cisco.com
CVE:	CVE-2004-1464
IPs:	192.168.103.2 - 2008-03-13 16:02

Check id:	1040070
Name:	Cisco IOS Vulnerability
Port:	161/udp - snmp
Risk factor:	Critical/Urgent
CVSS	9.3 (AV:N/AC:M/Au:N/C:C/I:C/A:C)
Family:	cisco
Description:	Stack-based buffer overflow in the Line Printer Daemon (LPD) in Cisco IOS before 12.2(18)SXF11, 12.4(16a), and 12.4(2)T6 allow remote attackers to execute arbitrary code by setting a long hostname on the target system, then causing an error message to be printed, as demonstrated by a telnet session to the LPD from a source port other than 515.
Solution:	Upgrade to a version of Cisco IOS that includes a fix to this problem
Reference:	url - http://www.cisco.com
CVE:	CVE-2007-5381
IPs:	192.168.103.2 - 2008-03-13 16:02

Check id:	1040070
Name:	Cisco IOS Vulnerability
Port:	161/udp - snmp
Risk factor:	Critical/Urgent
CVSS	9.3 (AV:N/AC:M/Au:N/C:C/I:C/A:C)
Family:	cisco
Description:	Stack-based buffer overflow in the Line Printer Daemon (LPD) in Cisco IOS before 12.2(18)SXF11, 12.4(16a), and 12.4(2)T6 allow remote attackers to execute arbitrary code by setting a long hostname on the target system, then causing an error message to be printed, as demonstrated by a telnet session to the LPD from a source port other than 515.
Solution:	Upgrade to a version of Cisco IOS that includes a fix to this problem
Reference:	url - http://www.cisco.com
CVE:	CVE-2007-5381
IPs:	192.168.103.2 - 2008-03-13 16:02

Check id:	1040070
Name:	Cisco IOS Vulnerability
Port:	161/udp - snmp
Risk factor:	Critical/Urgent
CVSS	9.3 (AV:N/AC:M/Au:N/C:C/I:C/A:C)
Family:	cisco
Description:	Stack-based buffer overflow in the Line Printer Daemon (LPD) in Cisco IOS before 12.2(18)SXF11, 12.4(16a), and 12.4(2)T6 allow remote attackers to execute arbitrary code by setting a long hostname on the target system, then causing an error message to be printed, as demonstrated by a telnet session to the LPD from a source port other than 515.
Solution:	Upgrade to a version of Cisco IOS that includes a fix to this problem
Reference:	url - http://www.cisco.com
CVE:	CVE-2007-5381
IPs:	192.168.103.2 - 2008-03-13 16:02

Check id:	1040110
Name:	Cisco IOS Vulnerability
Port:	161/udp - snmp
Risk factor:	Critical/Urgent
CVSS	9.3 (AV:N/AC:M/Au:N/C:C/I:C/A:C)
Family:	cisco
Description:	Cisco IOS 12.0 to 12.4 might allow remote attackers to execute arbitrary code via a heap-based buffer overflow in system timers. NOTE: this issue does not correspond to a specific vulnerability, rather a general weakness that only increases the feasibility of exploitation of any vulnerabilities that might exist. Such design-level weaknesses normally are not included in CVE, so perhaps this issue should be REJECTed.
Solution:	Upgrade to a version of Cisco IOS that includes a fix to this problem
Reference:	url - http://www.cisco.com
CVE:	CVE-2005-3481
IPs:	192.168.103.2 - 2008-03-13 16:02

Check id:	201198
Name:	Unencrypted remote management
Port:	23/tcp - telnet
Risk factor:	Critical/Urgent
CVSS	9.0 (AV:N/AC:L/Au:N/C:C/I:P/A:P)
Family:	remote-management
Description:	<p>The target is determined to use protocols such as HTTP, TELNET, rlogin, FTP, and SNMP for configuration management. These services can be accessed publicly, and are an invitation for malicious users to break in.</p> <p>These services are often susceptible to man-in-the middle attacks allowing for breaches of confidentiality as well as integrity, and give no confidentiality as well.</p>
Solution:	<p>In the case of rlogin and TELNET, you can switch to SSH.</p> <p>In the case of HTTP, it is suggested that you use SSL as an added layer of protection. SSH (a subset of it anyway, the SCP and SFTP protocols) can also be used to replace FTP.</p> <p>SNMP version 3, if configured correctly can also provide you with protection.</p>
IPs:	192.168.103.2 - 2008-03-13 16:02

Check id:	1040019
Name:	Cisco IOS Vulnerability
Port:	161/udp - snmp
Risk factor:	High
CVSS	7.8 (AV:N/AC:L/Au:N/C:N/I:N/A:C)
Family:	cisco
Description:	Cisco IOS allows remote attackers to cause a denial of service (crash) via a crafted IPv6 Type 0 Routing header.
Solution:	Upgrade to a version of Cisco IOS that includes a fix to this problem
Reference:	url - http://www.cisco.com
CVE:	CVE-2007-0481
IPs:	192.168.103.2 - 2008-03-13 16:02

Check id:	1040039
Name:	Cisco IOS Vulnerability
Port:	161/udp - snmp
Risk factor:	High
CVSS	7.8 (AV:N/AC:L/Au:N/C:N/I:N/A:C)
Family:	cisco
Description:	Cisco IOS 12.4 and earlier, when using the crypto packages and SSL support is enabled, allows remote attackers to cause a denial of service via a malformed (1) ClientHello, (2) ChangeCipherSpec, or (3) Finished message during an SSL session.
Solution:	Upgrade to a version of Cisco IOS that includes a fix to this problem
Reference:	url - http://www.cisco.com
CVE:	CVE-2007-2813
IPs:	192.168.103.2 - 2008-03-13 16:02

Check id:	1040053
Name:	Cisco IOS Vulnerability
Port:	161/udp - snmp
Risk factor:	High
CVSS	7.8 (AV:N/AC:L/Au:N/C:N/I:N/A:C)
Family:	cisco
Description:	Memory leak in the TCP listener in Cisco IOS 9.x, 10.x, 11.x, and 12.x allows remote attackers to cause a denial of service by sending crafted TCP traffic to an IPv4 address on the IOS device.
Solution:	Upgrade to a version of Cisco IOS that includes a fix to this problem
Reference:	url - http://www.cisco.com
CVE:	CVE-2007-0479
IPs:	192.168.103.2 - 2008-03-13 16:02

Check id:	113090
Name:	SNMP Agent Default Community Names
Port:	161/udp - snmp
Risk factor:	High
CVSS	7.5 (AV:N/AC:L/Au:N/C:P/I:P/A:P)
Family:	snmp
Description:	This SNMP server uses a common community name.
Information:	The remote SNMP server replies to the following default community strings: public
Solution:	Filter access to, or disable, the SNMP service
CVE:	CVE-1999-0517 CVE-1999-0516
Bugtraq:	11237 10576 177 2112 6825 7081 7212 7317 9681 986
IPs:	192.168.103.2 - 2008-03-13 16:02

Check id:	1040071
Name:	Cisco IOS Vulnerability
Port:	161/udp - snmp
Risk factor:	High
CVSS	7.5 (AV:N/AC:L/Au:N/C:P/I:P/A:P)
Family:	cisco
Description:	Cisco IOS 12.2T through 12.4 allows remote attackers to bypass Authentication, Authorization, and Accounting (AAA) RADIUS authentication, if the fallback method is set to none, via a long username.
Solution:	Upgrade to a version of Cisco IOS that includes a fix to this problem
Reference:	url - http://www.cisco.com
CVE:	CVE-2005-2105
IPs:	192.168.103.2 - 2008-03-13 16:02

Check id:	201332
Name:	Cisco IOS IKE Implementation XAUTH Bypass Vulnerability
Port:	161/udp - snmp
Risk factor:	High
CVSS	7.5 (AV:N/AC:L/Au:N/C:P/I:P/A:P)
Family:	cisco
Description:	Cisco IOS 12.2T, 12.3 and 12.3T, when processing an ISAKMP profile that specifies XAUTH authentication after Phase 1 negotiation, may not process certain attributes in the ISAKMP profile that specifies XAUTH, which allows remote attackers to bypass XAUTH and move to Phase 2 negotiations.
Reference:	solution - http://www.cisco.com/warp/public/707/cisco-sa-20050406-xauth.shtml
CVE:	CVE-2005-1058
IPs:	192.168.103.2 - 2008-03-13 16:02

Check id:	125860	
Name:	SNMP sysDesc Information	
Port:	161/udp - snmp	
Risk factor:	High	
CVSS	6.5 (AV:N/AC:L/Au:S/C:P/I:P/A:P)	
Family:	snmp	
Description:	It is possible to obtain the system information about the remote host by sending SNMP requests with the OID 1.3.6.1.2.1.1.1.	
Information:	System information	
	Field	Data
	sysDescr	Cisco Internetwork Operating System Software IOS (tm) C1700 Software (C1700-SV3Y-M), Version 12.2(4)YB, EARLY DEPLOYMENT RELEASE SOFTWARE (fc1) Synched to technology version 12.2(6.8)T2 TAC Support: http://www.cisco.com/tac Copyright (c) 1986-2002 by
	sysObjectID	.1.3.6.1.4.1.9.1.201
	sysUptime	(147643701) 17 days, 2:07:17.01
	sysName	thunderbluff
	sysServices	78
Solution:	Disable the SNMP service	
IPs:	192.168.103.2 - 2008-03-13 16:02	

Check id:	200217
Name:	ICMP Timestamp Request
Port:	General
Risk factor:	Medium
CVSS	5.0 (AV:N/AC:L/Au:N/C:N/I:P/A:N)
Family:	low level network testing
Description:	<p>The remote host replies to ICMP Timestamp requests.</p> <p>Knowing the exact time on your system may help an attacker to break time-based authentication systems.</p>
Solution:	Filter incoming ICMP type 13, and outgoing ICMP type 14 packets.
CVE:	CVE-1999-0524
IPs:	192.168.103.2 - 2008-03-13 16:02

Check id:	1040009
Name:	Cisco IOS Vulnerability
Port:	161/udp - snmp
Risk factor:	Medium
CVSS	5.0 (AV:N/AC:L/Au:N/C:N/I:N/A:P)
Family:	cisco
Description:	Cisco IOS 12.0 through 12.3YL, with BGP enabled and running the bgp log-neighbor-changes command, allows remote attackers to cause a denial of service (device reload) via a malformed BGP packet.
Solution:	Upgrade to a version of Cisco IOS that includes a fix to this problem
Reference:	url - http://www.cisco.com
CVE:	CVE-2005-0196
IPs:	192.168.103.2 - 2008-03-13 16:02

Check id:	1040078
Name:	Cisco IOS Vulnerability
Port:	161/udp - snmp
Risk factor:	Medium
CVSS	5.0 (AV:N/AC:L/Au:N/C:N/I:N/A:P)
Family:	cisco
Description:	Cisco IOS 12.0 through 12.2, when supporting SSH, allows remote attackers to cause a denial of service (CPU consumption) via a large packet that was designed to exploit the SSH CRC32 attack detection overflow (CVE-2001-0144).
Solution:	Upgrade to a version of Cisco IOS that includes a fix to this problem
Reference:	url - http://www.cisco.com
CVE:	CVE-2002-1024
IPs:	192.168.103.2 - 2008-03-13 16:02

Check id:	1040102
Name:	Cisco IOS Vulnerability
Port:	161/udp - snmp
Risk factor:	Medium
CVSS	5.0 (AV:N/AC:L/Au:N/C:N/I:N/A:P)
Family:	cisco
Description:	Secure Shell (SSH) 2 in Cisco IOS 12.0 through 12.3 allows remote attackers to cause a denial of service (device reload) (1) via a username that contains a domain name when using a TACACS+ server to authenticate, (2) when a new SSH session is in the login phase and a currently logged in user issues a send command, or (3) when IOS is logging messages and an SSH session is terminated while the server is sending data.
Solution:	Upgrade to a version of Cisco IOS that includes a fix to this problem
Reference:	url - http://www.cisco.com
CVE:	CVE-2005-1020
IPs:	192.168.103.2 - 2008-03-13 16:02

Check id:	1040102
Name:	Cisco IOS Vulnerability
Port:	161/udp - snmp
Risk factor:	Medium
CVSS	5.0 (AV:N/AC:L/Au:N/C:N/I:N/A:P)
Family:	cisco
Description:	Secure Shell (SSH) 2 in Cisco IOS 12.0 through 12.3 allows remote attackers to cause a denial of service (device reload) (1) via a username that contains a domain name when using a TACACS+ server to authenticate, (2) when a new SSH session is in the login phase and a currently logged in user issues a send command, or (3) when IOS is logging messages and an SSH session is terminated while the server is sending data.
Solution:	Upgrade to a version of Cisco IOS that includes a fix to this problem
Reference:	url - http://www.cisco.com
CVE:	CVE-2005-1020
IPs:	192.168.103.2 - 2008-03-13 16:02

Check id:	1040121
Name:	Cisco IOS Vulnerability
Port:	161/udp - snmp
Risk factor:	Medium
CVSS	5.0 (AV:N/AC:L/Au:N/C:N/I:N/A:P)
Family:	cisco
Description:	Cisco IOS 11.x and 12.0 through 12.2 allows remote attackers to cause a denial of service (traffic block) by sending a particular sequence of IPv4 packets to an interface on the device, causing the input queue on that interface to be marked as full.
Solution:	Upgrade to a version of Cisco IOS that includes a fix to this problem
Reference:	url - http://www.cisco.com
CVE:	CVE-2003-0567
IPs:	192.168.103.2 - 2008-03-13 16:02

Check id:	201334
Name:	Cisco IOS Secure Shell Server Denial of Service Vulnerability
Port:	161/udp - snmp
Risk factor:	Medium
CVSS	5.0 (AV:N/AC:L/Au:N/C:N/I:N/A:P)
Family:	cisco
Description:	Memory leak in Secure Shell (SSH) in Cisco IOS 12.0 through 12.3, when authenticating against a TACACS+ server, allows remote attackers to cause a denial of service (memory consumption) via an incorrect username or password.
Reference:	solution - http://www.cisco.com/warp/public/707/cisco-sa-20050406-ssh.shtml
CVE:	CVE-2005-1021
IPs:	192.168.103.2 - 2008-03-13 16:02

Check id:	125950
Name:	TCP SYN FIN
Port:	General
Risk factor:	Medium
CVSS	4.7 (AV:L/AC:H/Au:N/C:N/I:P/A:C) - This finding does not affect PASS/FAIL status for PCI.
Family:	low level network testing
Description:	<p>The TCP implementation on this host replies to invalid TCP packets. Packets with both the SYN and the FIN bit set are considered invalid and should be discarded.</p> <p>Not doing so could have a negative impact on IDS systems. Depending on the order in which the flag-bits are parsed, the TCP implementation of this host's operating system may see the SYN bit first and initiate a connection while the TCP implementation of the IDS parses the FIN bit first, making it believe that the connection has just been closed.</p> <p>Effectively, this could mean that a connection can be established without the IDS keeping track of it.</p>
Solution:	Contact your operating system vendor for a patch.
Reference:	<p>url - http://nvd.nist.gov/nvd.cfm?cvename=CVE-2007-3537</p> <p>url - http://www.kb.cert.org/vuls/id/464113</p> <p>url - http://archives.neohapsis.com/archives/bugtraq/2002-10/0266.html</p>
Bugtraq:	7487
IPs:	192.168.103.2 - 2008-03-13 16:02

Check id:	1040061
Name:	Cisco IOS Vulnerability
Port:	161/udp - snmp
Risk factor:	Medium
CVSS	4.6 (AV:L/AC:L/Au:N/C:P/I:P/A:P)
Family:	cisco
Description:	The TCL shell in Cisco IOS 12.2(14)S before 12.2(14)S16, 12.2(18)S before 12.2(18)S11, and certain other releases before 25 January 2006 does not perform Authentication, Authorization, and Accounting (AAA) command authorization checks, which may allow local users to execute IOS EXEC commands that were prohibited via the AAA configuration, aka Bug ID CSCeh73049.
Solution:	Upgrade to a version of Cisco IOS that includes a fix to this problem
Reference:	url - http://www.cisco.com
CVE:	CVE-2006-0485
IPs:	192.168.103.2 - 2008-03-13 16:02

Check id:	201260
Name:	Cisco IOS TCLSH AAA Command Authorization Bypass Vulnerability
Port:	161/udp - snmp
Risk factor:	Medium
CVSS	4.6 (AV:L/AC:L/Au:N/C:P/I:P/A:P)
Family:	cisco
Description:	The TCL shell in Cisco IOS 12.2(14)S before 12.2(14)S16, 12.2(18)S before 12.2(18)S11, and certain other releases before 25 January 2006 does not perform Authentication, Authorization, and Accounting (AAA) command authorization checks, which may allow local users to execute IOS EXEC commands that were prohibited via the AAA configuration, aka Bug ID CSCeh73049.
Reference:	solution - http://www.cisco.com/warp/public/707/cisco-sr-20060125-aaatcl.shtml
CVE:	CVE-2006-0485
Bugtraq:	16383
IPs:	192.168.103.2 - 2008-03-13 16:02

Check id:	125854								
Name:	Network Interfaces via SNMP								
Port:	161/udp - snmp								
Risk factor:	Medium								
CVSS	4.0 (AV:N/AC:L/Au:S/C:P/I:N/A:N)								
Family:	snmp								
Description:	It is possible to obtain the list of the network interfaces installed on the remote host by sending SNMP requests with the OID 1.3.6.1.2.1.2.1.0								
Information:	Interfaces <table><thead><tr><th>ifDescr</th><th>ifPhysAddress</th></tr></thead><tbody><tr><td>FastEthernet0</td><td>00:05:5e:2e:01:ab</td></tr><tr><td>Serial0</td><td>N/A</td></tr><tr><td>Null0</td><td>N/A</td></tr></tbody></table>	ifDescr	ifPhysAddress	FastEthernet0	00:05:5e:2e:01:ab	Serial0	N/A	Null0	N/A
ifDescr	ifPhysAddress								
FastEthernet0	00:05:5e:2e:01:ab								
Serial0	N/A								
Null0	N/A								
Solution:	Filter access to, or disable, the SNMP Service								
IPs:	192.168.103.2 - 2008-03-13 16:02								

Check id:	125862								
Name:	SNMP Open Port List								
Port:	161/udp - snmp								
Risk factor:	Medium								
CVSS	4.0 (AV:N/AC:L/Au:S/C:P/I:N/A:N)								
Family:	snmp								
Description:	A list of listening ports was obtained by querying the MIB on this host.								
Information:	Listening UDP ports								
	<table><thead><tr><th>Port</th><th>Destination Address</th></tr></thead><tbody><tr><td>161</td><td>192.168.103.2</td></tr><tr><td>162</td><td>192.168.103.2</td></tr><tr><td>67</td><td>192.168.103.2</td></tr></tbody></table>	Port	Destination Address	161	192.168.103.2	162	192.168.103.2	67	192.168.103.2
Port	Destination Address								
161	192.168.103.2								
162	192.168.103.2								
67	192.168.103.2								
Solution:	Filter access to, or disable, the SNMP service.								
IPs:	192.168.103.2 - 2008-03-13 16:02								

Check id:	1040084
Name:	Cisco IOS Vulnerability
Port:	161/udp - snmp
Risk factor:	Low
CVSS	2.1 (AV:L/AC:L/Au:N/C:N/I:N/A:P)
Family:	cisco
Description:	Cisco IOS 12.0 through 12.4 and IOS XR before 3.2, with IPv6 enabled, allows remote attackers on a local network segment to cause a denial of service (device reload) and possibly execute arbitrary code via a crafted IPv6 packet.
Solution:	Upgrade to a version of Cisco IOS that includes a fix to this problem
Reference:	url - http://www.cisco.com
CVE:	CVE-2005-2451
IPs:	192.168.103.2 - 2008-03-13 16:02

Check id:	201336
Name:	Cisco IOS IPv6 Processing Arbitrary Code Execution Vulnerability
Port:	161/udp - snmp
Risk factor:	Low
CVSS	2.1 (AV:L/AC:L/Au:N/C:N/I:N/A:P)
Family:	cisco
Description:	Cisco IOS 12.0 through 12.4 and IOS XR before 3.2, with IPv6 enabled, allows remote attackers on a local network segment to cause a denial of service (device reload) and possibly execute arbitrary code via a crafted IPv6 packet.
Reference:	solution - http://www.cisco.com/warp/public/707/cisco-sa-20050729-ipv6.shtml
CVE:	CVE-2005-2451
Bugtraq:	14414
IPs:	192.168.103.2 - 2008-03-13 16:02

Check id:	125472
Name:	Relative IP identification numbers
Port:	General
Risk factor:	Low
CVSS	1.0
Family:	low level network testing
Description:	<p>The operating system running on this host uses a weak algorithm for selecting IP ID numbers. This enables a potential attacker to predict subsequent IP ID values.</p> <p>A range of problems comes with this, such as an attacker being able to use this host as a zombie when port scanning, or being able to keep track of the amount of requests made to this server over a period of time.</p>
Solution:	Contact your operating system vendor for a patch.
IPs:	192.168.103.2 - 2008-03-13 16:02

Check id:	125993
Name:	Traceroute
Port:	General
Risk factor:	Low
CVSS	0.0
Family:	Information gathering
Description:	<p>This check tries to determine the path; traceroute, between our attacker and your target host. This path may give an attacker valuable information about through which routers; hops, traffic passes through. This is not a vulnerability in itself it is merely considered information, however, an attacker could possibly use this information to determine what ISP you have and so forth.</p> <p>Note: The path is not static and will most likely change depending on from which host you perform the traceroute. There is also no way you can fix this problem as it involves changing configurations on all the hops along the way.</p>
Information:	host[:dport]/protocol (2 hops) 1 192.168.200.235:53/udp 2 192.168.103.2:53/udp [closed]
IPs:	192.168.103.2 - 2008-03-13 16:02

Check id:	200839		
Name:	Operating System Detection		
Port:	General		
Risk factor:	Low		
CVSS	0.0		
Family:	fingerprint		
Description:	This check attempts to identify the running Operating System of the scanned host.		
Information:	Operating System Guess	Based on Service/Protocol	Accuracy Estimation
	Cisco IOS 12.2(4)YB	snmp	100
IPs:	192.168.103.2 - 2008-03-13 16:02		

Check id:	100011
Name:	VHost Settings
Port:	General
Risk factor:	Low
CVSS	0.0
Family:	settings
Description:	The following virtual hosts have been disabled.
Information:	Unresolvable virtual hosts: nej.ja
IPs:	192.168.103.2 - 2008-03-13 16:02

Check id:	201333
Name:	Cisco AAA Command Authorization by-pass
Port:	161/udp - snmp
Risk factor:	Low
CVSS	0.0
Family:	cisco
Description:	A vulnerability exists within Cisco Internetwork Operating System (IOS) Authentication, Authorization, and Accounting (AAA) command authorization feature, where command authorization checks are not performed on commands executed from the Tool Command Language (Tcl) exec shell. This may allow authenticated users to bypass command authorization checks in some configurations resulting in unauthorized privilege escalation.
Reference:	solution - http://www.cisco.com/warp/public/707/cisco-sr-20060125-aaatcl.shtml
IPs:	192.168.103.2 - 2008-03-13 16:02

Check id:	201335
Name:	Cisco IOS Software Processing of SAA Packets
Port:	161/udp - snmp
Risk factor:	Low
CVSS	0.0
Family:	cisco
Description:	The Service Assurance Agent (SAA) in Cisco IOS 12.0 through 12.2, aka Response Time Reporter (RTR), allows remote attackers to cause a denial of service (crash) via malformed RTR packets to port 1967.
Reference:	solution - http://www.cisco.com/warp/public/707/cisco-sa-20030515-saa.shtml
IPs:	192.168.103.2 - 2008-03-13 16:02

Check id:	300211
Name:	Cisco IOS Version
Port:	161/udp - snmp
Risk factor:	Low
CVSS	0.0
Family:	cisco
Description:	Outscan has determined that this device is a Cisco device with the IOS operating system.
Information:	Cisco IOS version: 12.2(4)YB
IPs:	192.168.103.2 - 2008-03-13 16:02