

Vulnerability Statistics

Reasons for PCI Failure	
•	12 Systems found to be non-compliant due to failing vulnerabilities.
•	1 System had a mismatched hostname on its SSL certificate.

Scan Type	Enterprise	Report Generated	08-Jun-11 11:13
Systems Scanned	20	Start Date	13-Apr-11 11:54
New Systems	2	End Date	16-Apr-11 16:32

21	High risk vulnerabilities found.	9	Systems (45%) had high risk vulnerabilities.
29	Medium risk vulnerabilities found.	3	Systems (15%) had medium risk vulnerabilities.
16	Low risk vulnerabilities found.	0	Systems (0%) had low risk vulnerabilities.
16	SANS vulnerabilities found.	9	Systems (45%) had SANS vulnerabilities.
22	New vulnerabilities found.	12	Systems (60%) had vulnerabilities.
1	Urgent vulnerabilities found.	8	Systems (40%) had no vulnerabilities.
4	Overdue vulnerabilities found.	1	Systems (5%) had urgent vulnerabilities.
		3	Systems (15%) had overdue vulnerabilities.

Key	Increase	No change	Decrease	High Risk	Medium Risk	Low Risk	No Services	No Ports/Vulns
-----	----------	-----------	----------	-----------	-------------	----------	-------------	----------------

Systems

Host Name	IP Address	Critical	Ports	Vulnerabilities
www.your_company.nl	192.168.0.103		7	13 (7 New)
www.yourcompany.co.uk	192.168.0.100		5	9 (5 New)
www.example.com	192.168.0.112		3	11 (4 New)
dns0.example.com	192.168.0.110		5	5 (1 New)
mail.example.com	192.168.0.111		8	5
sql1.manc.yourcompany.com	192.168.1.52		3	4
sql2.manc.yourcompany.com	192.168.1.53		2	4
www.yourcompany.com	192.168.0.101		12	2 (2 New)
www.your_company.fr	192.168.0.105		5	3 (3 New)
www.yourcompany.net	192.168.0.102		2	5
apollo.example.com	192.168.0.81		3	3
www.yourcompany.com.my	192.168.0.106		2	2
www1.manc.yourcompany.com	192.168.1.54		2	0
www2.manc.yourcompany.com	192.168.1.55		2	0
mail1.manc.yourcompany.com	192.168.1.50		1	0
mail2.manc.yourcompany.com	192.168.1.51		1	0
192.168.0.104	192.168.0.104		2	0
gopher.example.com	192.168.0.93		0	0
192.168.100.9	192.168.100.9		1	0
laptop.yourcompany.com	192.168.0.57		0	0

All Vulnerabilities

Frequency	Vulnerability	Severity
6	High Risk Ports Open	High Risk
3	SNMP Default Community Names SANS	High Risk
1	IIS WebDAV Buffer Overrun	High Risk
1	MySQL Database Accessible Without Password LATE	High Risk
1	Administration Interface with Weak Password New	High Risk
1	Possible Compromise New	High Risk
1	BIND < 8.2.3 Buffer Overrun SANS LATE	High Risk
1	Authentication Bypass Through Cookie Manipulation New	High Risk
1	Apache < 1.3.26 Chunked Encoding Vulnerability SANS	High Risk
1	IIS ASP.NET Application Trace Enabled New	High Risk
1	Sendmail < 8.12.8 Buffer Overrun SANS URGENT	High Risk
1	Sensitive Information Leakage New	High Risk
1	Script Appears Vulnerable to SQL Injection New	High Risk
1	Script Allows Arbitrary Command Execution New	High Risk
3	Globally Useable Name Server SANS	Medium Risk
2	Apache < 1.3.27 Multiple Vulnerabilities	Medium Risk
2	Cross-Site Scripting	Medium Risk
2	SSH Protocol Version 1 Enabled	Medium Risk
2	MySQL < 3.23.58, 4.0.15 Password Overflow SANS	Medium Risk
2	MySQL < 3.23.56 Privilege Escalation SANS	Medium Risk
1	OpenSSH < 3.6.1p2 PAM Timing Attack	Medium Risk
1	Lotus Domino < 5.0.9 Database Lock DoS	Medium Risk
1	MySQL < 3.23.55 Multiple Vulnerabilities SANS	Medium Risk
1	SMTP Server Allows VRFY/EXPN	Medium Risk
1	Script Allows Arbitrary Redirection New	Medium Risk
1	Apache < 1.3.31, 2.0.49 Multiple Vulnerabilities SANS	Medium Risk
1	XPath Injection New	Medium Risk
1	Lotus Domino Anonymous Database Access	Medium Risk
1	OpenSSL < 0.9.6m, 0.9.7d Multiple Vulnerabilities SANS	Medium Risk
1	Weak or Ineffective Authentication Mechanism New	Medium Risk
1	SSL Certificate Problems New	Medium Risk
1	IIS global.asa Accessible	Medium Risk
1	Apache mod_ssl < 2.8.10 off by one Vulnerability	Medium Risk
1	IIS .printer ISAPI Filter Enabled	Medium Risk
1	DNS Zone Transfer LATE	Medium Risk
1	Service Permits Unauthenticated Users to Send Arbitrary Emails New	Medium Risk
4	Holes Detected in Firewall Configuration	Low Risk
3	TRACE and/or TRACK Methods Enabled	Low Risk
2	DNS Cache Snooping	Low Risk
2	Apache < 1.3.29 Multiple Local Flaws	Low Risk
1	NTP Information Leakage New	Low Risk
1	Apache mod_userdir Information Leak	Low Risk
1	Microsoft Frontpage Extensions Installed	Low Risk

Frequency	Vulnerability	Severity
1	Private IP Address Leakage	Low Risk
1	Script Calling phpinfo() Detected LATE	Low Risk