McAfee | McAfee SECURE™

Executive Report

Softlayer Technologies, Inc.

13-JAN-2010 15:36

Confidential Information
The following report contains confidential information. Do not distribute, email, fax or transfer via any electric mechanism unless it has been approved by your organization's security policy. All copies and backups of this document should be maintained on protected storage at all times. Do not share any of the information contained within this report with anyone unless you confirm they are authorized to view the information.

Disclaimer
This, or any other, vulnerability audit cannot and does not guarantee security. McAfee makes no warranty or claim of any kind, whatsoever, about the accuracy or usefulness of any information provided herein. By using this information you agree that McAfee shall be held harmless in any event. McAfee makes this information available solely under its Terms of Service Agreement published at www.mcafeesecure.com.

Executive Summary

This report was generated by PCI Approved scanning vendor, McAfee, under certificate number 3709-01-03 in the framework of the PCI data security initiative.

As a Qualified Independent Scan Vendor McAfee is accredited by Visa, MasterCard, American Express, Discover Card and JCB to perform network security audits conforming to the Payment Card Industry (PCI) Data Security Standards.

To earn validation of PCI compliance, network devices being audited must pass tests that probe all of the known methods hackers use to access private information, in addition to vulnerabilities that would allow malicious software (i.e. viruses and worms) to gain access to or disrupt the network devices being tested.

NOTE: In order to demonstrate compliance with the PCI Data Security Standard a vulnerability scan must have been completed within the past 90 days with no vulnerabilities listed as URGENT, CRITICAL or HIGH (numerical severity ranking of 3 or higher) present on any device within this report. Additionally, Visa and MasterCard regulations require that you configure your scanning to include all IP addresses, domain names, DNS servers, load balancers, firewalls or external routers used by, or assigned to, your company, and that you configure any IDS/IPS to not block access from the originating IP addresses of our scan servers.

Certification of Regulatory Compliance

Sites are tested and certified daily to meet all U.S. Government requirements for remote vulnerability testing as set forth by the National Infrastructure Protection Center (NIPC). They are also certified to meet the security scanning requirements of Visa USA's
Cardholder Information Security Program (CISP), Visa International's Account Information Security (AIS) program, MasterCard Internationals's Site Data Protection (SDP) program, American Express' CID security program, the Discover Card Information Security and
Compliance (DISC) program within the framework of the Payment Card Industry (PCI) Data Security Standard.

Compliance Glossary

McAfee Secure

Signifies device, as of the date of this report, is compliant with the McAfee SECURE certification.

Network devices certified as McAfee Secure are tested daily and certified to pass all external vulnerability audit recommendations of the Department of Homeland Security's National Infrastructure Protection Center (NIPC) and the requirements of the Payment Card Industry Data Security Standard (PCI-DSS). McAfee Secure certification also meets the requirements for network vulnerability audits of the CHILDREN'S ONLINE PRIVACY PROTECTION ACT OF 1998, the HEALTH INSURANCE PORTABILITY AND ACCOUNTABILITY ACT OF 1996 (HIPAA), the GRAMM-LEACH-BAILEY ACT (GLBA) protecting financial information, and the SARBANES-OXLEY ACT (SOX).

Payment Card Industry (PCI) Data Security Standard

PCI COMPLIANCE - Signifies device, as of the date of this report, is compliant with the remote vulnerability audit requirements of the Payment Card Industry Data Security Standard (PCI-DSS), Visa USA's Cardholder Information Security Program (CISP), Visa International's Account Information Security (AIS) program, MasterCard International's Site Data Protection (SDP) program, the American Express Data Security Standards (DSS), and Discover Card's DISC program.

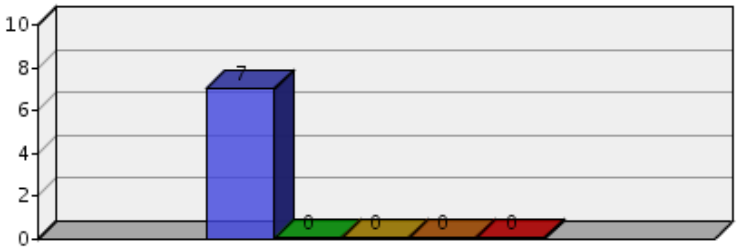
Report Overview

Customer Name	Softlayer Technologies, Inc.
Date Generated	13-JAN-2010 15:36
Report Type	Executive
Devices	2
Device Groups	0
Vulnerabilities	5

Report Contents

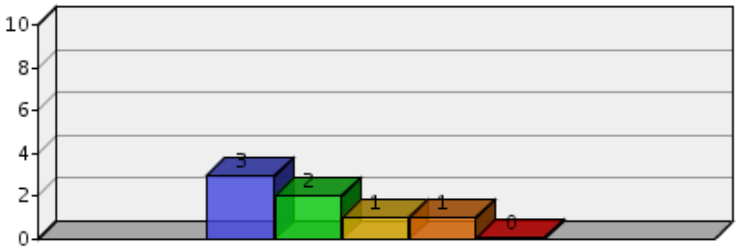
Vulnerabilities By Severity - All 2 Devices

	Severity
0	Urgent
0	Critical
0	High
0	Medium
7	Low



Vulnerabilities By Category (Top 5) - All 2 Devices

	Category
3	Other
2	Web Server
1	Information Gathering
1	Web Application
0	



Device Compliance

Name	McAfee Secure	SDP
manage.softlayer.com	Pass	Pass
www.softlayer.com	Pass	Pass

Device Overview

Name	Urgent	Critical	High	Medium	Low	Open Ports
manage.softlayer.com	0	0	0	0	5	2
www.softlayer.com	0	0	0	0	2	3

Vulnerability Levels

Severity	Level	Description
5	Urgent	Intruders can easily gain control of the device being tested, which can lead to the compromise of your entire network security. Or hackers can use this device to access sensitive information from other devices in your network. Hackers are often actively scanning for this type of vulnerability. For example, vulnerabilities at this level may include full read and write access to files or databases, remote execution of commands, gaining Administrator or Root level access, and the presence of Trojans or backdoors.
4	Critical	Intruders can possibly gain direct control of the device being tested, or there may be potential leakage of highly sensitive information. For example, vulnerabilities at this level may include full read access to files, potential backdoors, or a listing of all the users hosted on the device.
3	High	Intruders may be able to gain access to specific information stored on the device being tested, including security settings. This could result in potential misuse of, or unauthorized access to the device or information stored on it. For example, vulnerabilities at this level may include partial disclosure of file contents, access to certain files on the host, directory browsing, disclosure of filtering rules and security mechanisms, denial of service attacks, and unauthorized use of services such as mail-relaying.
2	Medium	Intruders may be able to collect sensitive information from the host, such as the precise version of OS or software installed or directory structure. While this level of vulnerability is not directly exploitable itself, with this information intruders can more easily exploit possible vulnerabilities specific to software versions in use.
1	Low	Intruders can collect general information about the device being tested (open ports, OS or software type, etc.). Hackers may be able to use this information to find exploitable vulnerabilities.