

## Security Report - By Device

Secured Financial Network, Inc.

04-OCT-2007 11:11

### **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. ScanAlert 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 ScanAlert shall be held harmless in any event. ScanAlert makes this information available solely under its Terms of Service Agreement published at [www.scanalert.com](http://www.scanalert.com).

## Executive Summary

This report was generated by the SDP compliant scanning vendor ScanAlert, under certificate number 3709-01-01 in the framework of the PCI data security initiative and took into consideration security requirements as expressed in the MasterCard SDP Security Standard.

As a "Qualified Independent Scan Vendor" ScanAlert 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.

## ScanAlert's Certification of Regulatory Compliance

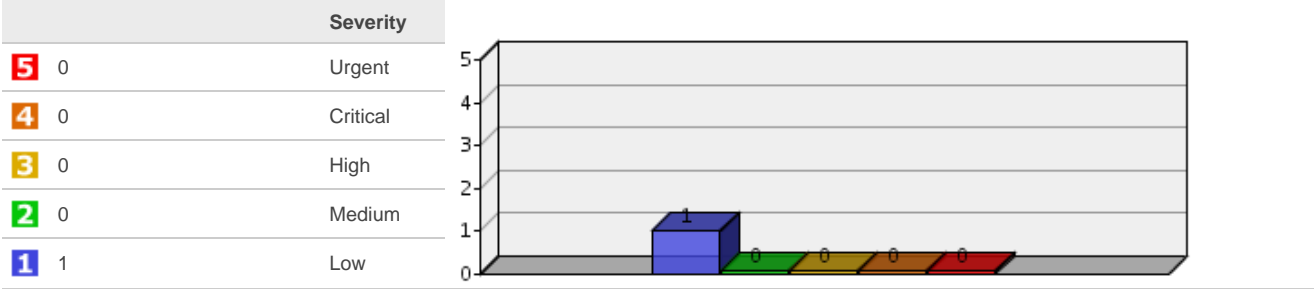
HACKER SAFE sites are tested and certified daily by ScanAlert to meet all U.S. Government requirements for remote vulnerability testing as set forth by the National Infrastructure Protection Center (NIPC) and are accredited by the SANS Institute to meet the requirements of the SANS/FBI "Top Twenty Internet Security Vulnerabilities" test. 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 International'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.

Report Overview	Report Contents
-----------------	-----------------

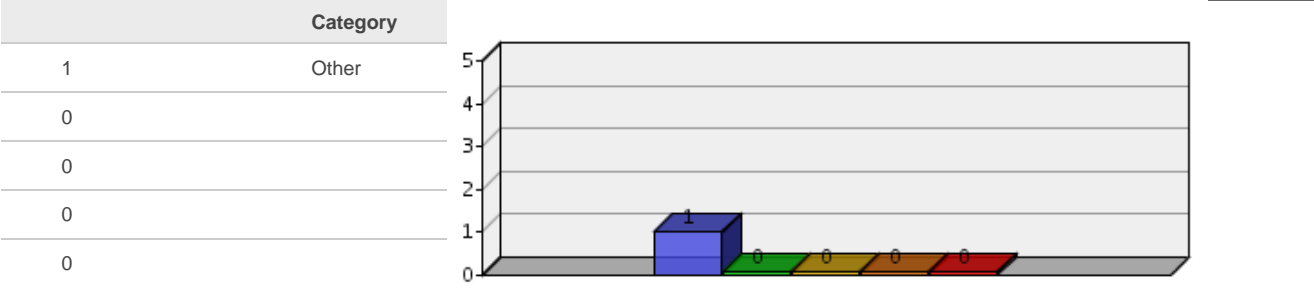
<b>Customer Name</b>	Secured Financial Network, Inc.
<b>Date Generated</b>	04-OCT-2007 11:11
<b>Report Type</b>	Security - By Device
<b>Devices</b>	1
<b>Device Groups</b>	0
<b>Vulnerabilities</b>	1

- Vulnerabilities By Severity
- Vulnerabilities By Category
- Device Overview
- Services Detected
- All Vulnerabilities Found
- Device Detail
- Appendix

### Vulnerabilities By Severity



### Vulnerabilities By Category (Top 5)








### Services Detected - All 1 Devices

Port	Protocol	Service		Devices
443	tcp	https		1

## All Vulnerabilities Found

Name	Category	Devices
<b>1</b> OS Identification	Other	1

## Device Overview

Name	 Urgent	 Critical	 High	 Medium	 Low	Open Ports
208.69.229.228	0	0	0	0	1	1

## Overview - 208.69.229.228

Last Audit Date	5 Urgent	4 Critical	3 High	2 Medium	1 Low	Total
06-SEP-2007 14:41	0	0	0	0	1	1

## Open Ports - 208.69.229.228

Port	Protocol	Service	Banner
443	tcp	https	tlsv1

## Vulnerabilities - 208.69.229.228

## Information Disclosures - 208.69.229.228

### 1 OS Identification

Port	First Detected	Category
0	06-SEP-2007 10:38	Other
Protocol	Fix Difficulty	Impact
ICMP	Medium	Information Disclosure

#### Description

This test attempts to identify the Operating System type and version by sending modified ICMP requests using the techniques outlined in Ofir Arkin's paper 'ICMP Usage In Scanning'.

An attacker may use this technique to try and identify the remote operating system.

#### Solution

Create a filtering policy for the ICMP types you use and block all other types.

#### Result

Remote operating system : Microsoft Windows 2003 Server  
Confidence Level : 75  
Method : HTTP

The remote host is running Microsoft Windows 2003 Server

#### Links

[ICMP Usage In Scanning](#)

#### Related

None

None

## Resolved Items - 208.69.229.228

None

## Vulnerability Levels

Severity	Level	Description
5	Urgent	<p>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.</p> <p>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.</p>
4	Critical	<p>Intruders can possibly gain direct control of the device being tested, or there may be potential leakage of highly sensitive information.</p> <p>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.</p>
3	High	<p>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.</p> <p>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.</p>
2	Medium	<p>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.</p>
1	Low	<p>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.</p>