



ASV Scan Report - Attestation of Scan Compliance

1. Scan Customer Information

Company: Angela Williams	Contact Name: Angela Williams Miller
Job Title: Administrator	Telephone: 352-480-9856
E-mail: anc.electronics.n.more@gmail.com	Business Address: 5253 Southeast 38th Street
City: Ocala	State/Province: FL
Country:	ZIP: 34480
	URL:

2. Approved Scanning Vendor Information

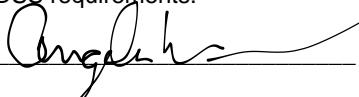
Company: SAINT Corporation	Contact Name: SAINT ASV Staff
Job Title: IT Security Consultant	Telephone: 301-656-0521
E-mail: asvstaff@saintcorporation.com	Business Address: 10440 Little Patuxent Pkwy 12th Floor
City: Columbia	State/Province: MD
Country: US	ZIP: 21044
	URL: http://www.saintcorporation.com

3. Scan Status

Date scan completed: Feb. 5, 2026	Scan expiration date (90 days from scan date): May 6, 2026
Compliance Status: PASS	Scan Report Type: Full scan
Number of unique in-scope components scanned: 1	Number of identified failing vulnerabilities: 0
Number of components found by ASV but not scanned because scan customer confirmed they were out of scope: 0	

4. Scan Customer Attestation

Angela Williams attests on February 5, 2026 that this scan (either by itself or combined with multiple, partial, or failed scans/rescans, as indicated in the above Section 3, "Scan Status") includes all components which should be in scope for PCI DSS, any component considered out of scope for this scan is properly segmented from my cardholder data environment, and any evidence submitted to the ASV to resolve scan exceptions including compensating controls if applicable is accurate and complete. Angela Williams also acknowledges 1) accurate and complete scoping of this external scan is my responsibility, and 2) this scan result only indicates whether or not my scanned systems are compliant with the external vulnerability scan requirement of PCI DSS; this scan result does not represent my overall compliance status with PCI DSS or provide any indication of compliance with other PCI DSS requirements.

Signature:  Name: Angela Williams Title: CEO/owner

5. ASV Attestation

This scan and report was prepared and conducted by SAINT Corporation under certificate number 4268-01-18, according to internal processes that meet PCI DSS Requirement 11.3.2 and the ASV Program Guide.

SAINT Corporation attests that the PCI DSS scan process was followed, including a manual or automated Quality Assurance process with customer boarding and scoping practices, review of results for anomalies, and review and correction of 1) disputed or incomplete results, 2) false positives, 3) compensating controls (if applicable), and 4) active scan interference. This report and any exceptions were reviewed by SAINT ASV Staff.

Scan Session: mID821954; Scan Policy: PCI External; Scan Data Set: 5 February 2026 10:35

Copyright 2001-2026 SAINT Corporation. All rights reserved.



SAINTwriter Assessment Report

Report Generated: February 5, 2026

1 Introduction

On February 5, 2026, at 10:35 AM, a PCI External assessment was conducted using the SAINT 10.6.46 vulnerability scanner. The scan discovered a total of one live host, and detected zero critical problems, zero areas of concern, and zero potential problems. The hosts and problems detected are discussed in greater detail in the following sections.

2 Summary

The following vulnerability severity levels are used to categorize the vulnerabilities:

CRITICAL PROBLEMS

Vulnerabilities which pose an immediate threat to the network by allowing a remote attacker to directly gain read or write access, execute commands on the target, or create a denial of service.

AREAS OF CONCERN

Vulnerabilities which do not directly allow remote access, but do allow privilege elevation attacks, attacks on other targets using the vulnerable host as an intermediary, or gathering of passwords or configuration information which could be used to plan an attack.

POTENTIAL PROBLEMS

Warnings which may or may not be vulnerabilities, depending upon the patch level or configuration of the target. Further investigation on the part of the system administrator may be necessary.

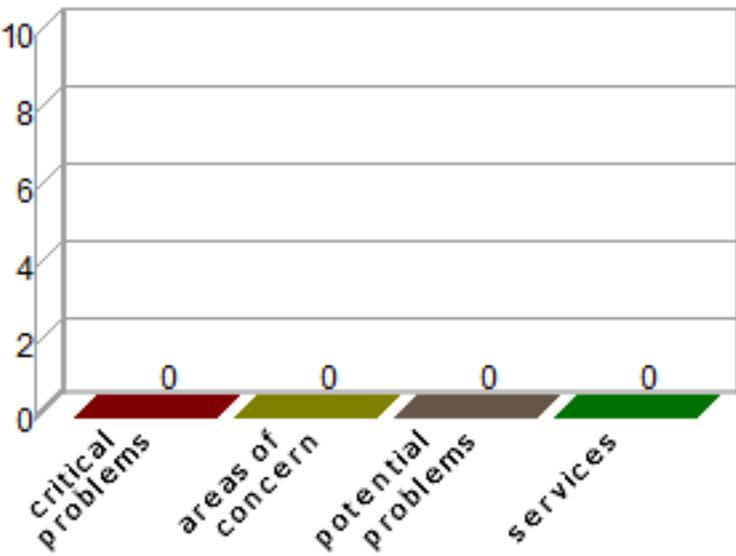
SERVICES

Network services which accept client connections on a given TCP or UDP port. This is simply a count of network services, and does not imply that the service is or is not vulnerable.

The sections below summarize the results of the scan.

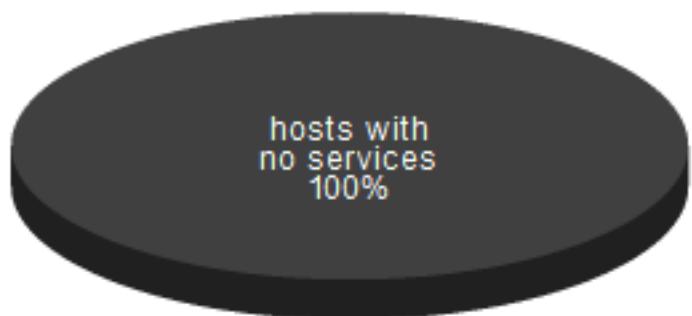
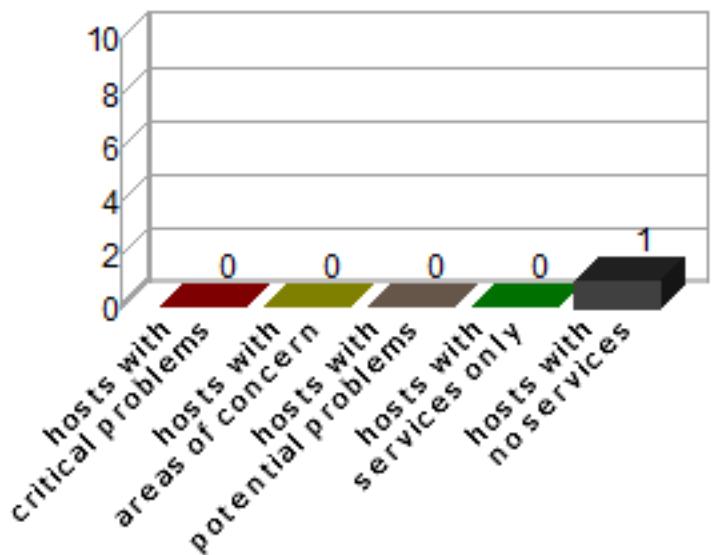
2.1 Vulnerabilities by Severity

This section shows the overall number of vulnerabilities and services detected at each severity level.



2.2 Hosts by Severity

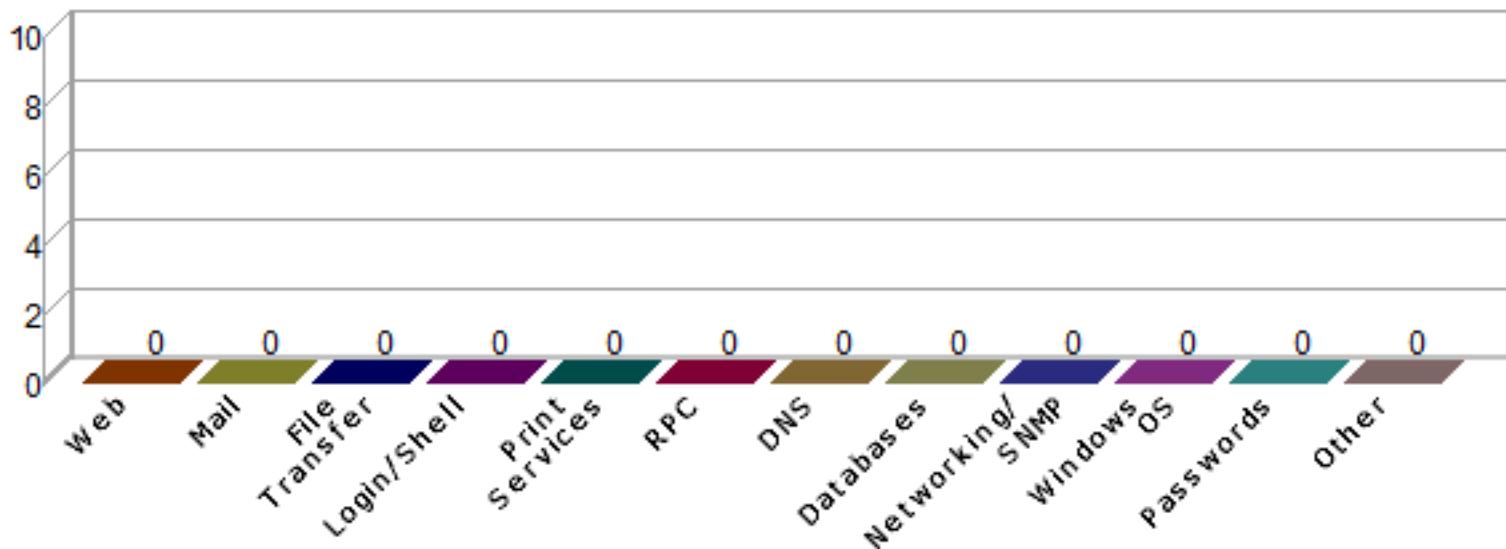
This section shows the overall number of hosts detected at each severity level. The severity level of a host is defined as the highest vulnerability severity level detected on that host.



2.3 Vulnerabilities by Class

This section shows the number of vulnerabilities detected in each vulnerability class.

Class	Description
Web	Vulnerabilities in web servers, CGI programs, and any other software offering an HTTP interface
Mail	Vulnerabilities in SMTP, IMAP, POP, or web-based mail services
File Transfer	Vulnerabilities in FTP and TFTP services
Login/Shell	Vulnerabilities in ssh, telnet, rlogin, rsh, or rexec services
Print Services	Vulnerabilities in lpd and other print daemons
RPC	Vulnerabilities in Remote Procedure Call services
DNS	Vulnerabilities in Domain Name Services
Databases	Vulnerabilities in database services
Networking/SNMP	Vulnerabilities in routers, switches, firewalls, or any SNMP service
Windows OS	Missing hotfixes or vulnerabilities in the registry or SMB shares
Passwords	Missing or easily guessed user passwords
Other	Any vulnerability which does not fit into one of the above classes



3 Overview

The following tables present an overview of the hosts discovered on the network and the vulnerabilities contained therein.

3.1 Host List

This table presents an overview of the hosts discovered on the network.

Host Name	Netbios Name	IP Address	Host Type	Critical Problems	Areas of Concern	Potential Problems
47.223.152.161		47.223.152.161		0	0	0

3.2 Vulnerability List

This table presents an overview of the vulnerabilities detected on the network.

Host Name	Severity	Vulnerability / Service	Class	CVE	Exploit Available?
47.223.152.161		nothing to report			

4 Details

The following sections provide details on the specific vulnerabilities detected on each host.

4.1 47.223.152.161

IP Address: 47.223.152.161

Scan time: Feb 05 10:35:11 2026

nothing to report

Scan Session: mID821954; Scan Policy: PCI External; Scan Data Set: 5 February 2026 10:35

Copyright 2001-2026 SAINT Corporation. All rights reserved.



ASV Scan Report Executive Summary

Report Generated: February 5, 2026

Part 1. Scan Information

Scan Customer Company: Angela Williams
Date scan was completed: February 5, 2026

ASV Company: SAINT Corporation
Scan expiration date: May 6, 2026

Part 2. Component Compliance Summary

Host Name	PCI Compliant?
47.223.152.161	PASS

Part 3a. Vulnerabilities Noted for each Component

Component:Port	Vulnerability / Service	CVE	PCI Severity	CVSS Base Score	PCI Compliant?	Exceptions, False positives, or Compensating Controls Noted by the ASV for this Vulnerability
47.223.152.161	nothing to report					

Part 3b. Special Notes to Scan Customer by Component

Component	Special Note to Scan Customer	Item Noted	Per section 7.2 of the ASV Program Guide, scan customer's description of action taken and declaration that software is either needed for business and implemented securely, or removed.
-----------	-------------------------------	------------	---

Part 3c. Special Notes - Full Text

Part 4a. Scope Submitted by Scan Customer for Discovery

- 47.223.152.161

Part 4b. Scan Customer Designated "In-Scope" Components (Scanned)

- 47.223.152.161

Part 4c. Scan Customer Designated "Out-of-Scope" Components (Not Scanned)

No out-of-scope components were found.

Scan Session: mID821954; Scan Policy: PCI External; Scan Data Set: 5 February 2026 10:35

Copyright 2001-2026 SAINT Corporation. All rights reserved.