Aperia - ASV Scan Report Summary

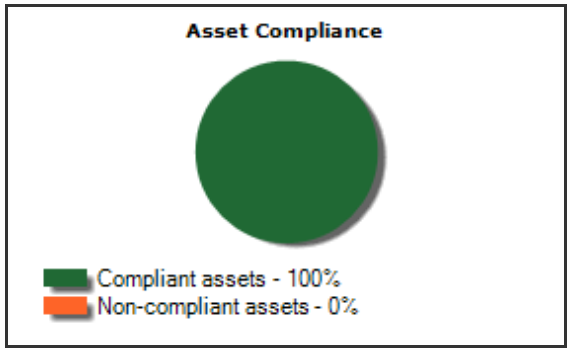
TURNERS INTERNATIONAL TRAVEL SERVICE

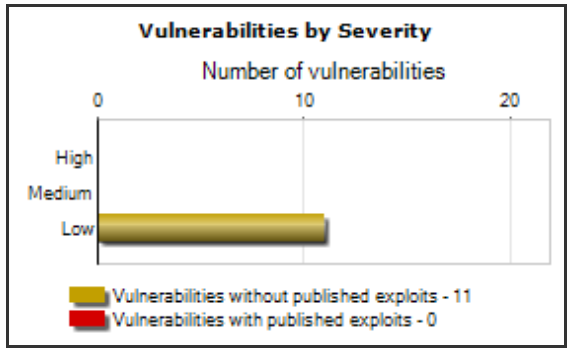
Audited on August 02, 2023. Reported on August 03, 2023

Part 1. Scan Information

Scan Customer Company: TURNERS INTERNATIONAL TRAVEL SERVICE	ASV Company: Aperia
Date scan was completed: August 2, 2023	Scan expiration date: October 31, 2023

Asset and Vulnerabilities Compliance Overview





Part 2. Component Compliance Summary

41.162.84.70	PASS

Part 3a. Vulnerabilities Noted for each Component

Part 3a-1.1. 41.162.84.70

Component	Vulnerabilities Noted per Component	Severity Level	CVSS Score	Compliance Status	Exceptions, False Positives, or Compensating Controls Noted by the ASV for this Vulnerability
41.162.84.70	45006 - Traceroute	Low	0.0	PASS	The vulnerability is not included in the NVD
41.162.84.70	45004 - Target Network Information	Low	0.0	PASS	The vulnerability is not included in the NVD
41.162.84.70	82040 - ICMP Replies Received	Low	0.0	PASS	The vulnerability is not included in the NVD
41.162.84.70	82004 - Open UDP Services List	Low	0.0	PASS	The vulnerability is not included in the NVD
41.162.84.70	6 - DNS Host Name	Low	0.0	PASS	The vulnerability is not included in the NVD
41.162.84.70	45005 - Internet Service Provider	Low	0.0	PASS	The vulnerability is not included in the NVD
41.162.84.70	34011 - Firewall Detected	Low	0.0	PASS	The vulnerability is not included in the NVD
41.162.84.70	45426 - Scan Activity per Port	Low	0.0	PASS	The vulnerability is not included in the NVD
41.162.84.70	45039 - Host Names Found	Low	0.0	PASS	The vulnerability is not included in the NVD
41.162.84.70	45038 - Host Scan Time - Scanner	Low	0.0	PASS	The vulnerability is not included in the NVD
41.162.84.70	42017 - Remote Access or Management Service Detected	Low	0.0	PASS	The vulnerability is not included in the NVD

Part 3a-1.2. Consolidated Solution/Correction Plan for the above Component:

For

These vulnerabilities can be resolved by performing the following 2 steps.

Vulnerability	Remediation Step
Open UDP Services List	Shut down any unknown or unused service on the list. If you have difficulty working out which service is provided by which process or program, contact your provider's support team. For more information about commercial and open-source Intrusion Detection Systems available for detecting port scanners of this kind, visit the CERT Web site.
Remote Access or Management Service Detected	Expose the remote access or remote management services only to the system administrators or intended users of the system.

Part 3b. Special Notes by Component

Part 3b-1. 41.162.84.70

Component	Special Note	Item Noted	Scan Customer's description of action taken and declaration that software is either implemented securely or removed
41.162.84.70	Remote Access	Remote Access Service name: ISAKMP on UDP port 500.	I confirm that the software is required and is implemented securely

Part 3c. Special Notes - Full Text

Remote Access
Special Note to Scan Customer: Due to increased risk to the cardholder data environment when remote access software is present, 1) justify the business need for this software to the ASV and confirm it is implemented securely, or 2) confirm it is disabled/removed. Consult your ASV if you have questions about this Special Note.

Part 4a. Scan Scope Submitted by Scan Customer for discovery

41.162.84.70

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

41.162.84.70

Part 4c. Scan Customer Designated "Out-Of-Scope" components (Not Scanned)