AFRITECH
CYBER SECURITY CONSULTING

// CONFIDENTIAL

> SECURITY ASSESSMENT REPORT

VULNERABILITY SCANNING AND PENETRATION TESTING REVIEW

PREPARED FOR

Meridian Payments (Pty) Ltd

REPORT NUMBER	REPORT DATE	CLASSIFICATION
AFR-PEN-2026-014	30 October 2026	Confidential

Afritech Computing (Pty) Ltd

Corporate Park North, 64 Roan Cres, Randjespark, Midrand, 1685, South Africa

cybersecurity@afriteq.co.za

Important Disclaimer

This report is supplied on the basis that it is for the sole use of the parties listed and to whom it is addressed, and exclusively for the objectives set out herein.

No party, other than those specified, may rely on this report for any purpose whatsoever.

Afritech Computing (Pty) Ltd ("Afritech") does not accept any liability or responsibility towards any third party to whom this report is shown or into whose hands it may fall.

This report should not be relied upon for any assurances in relation to third parties and/or activities that are not covered by the agreed scope of work described in this report. All such other parties and activities are outside the scope of this report and have therefore not been reviewed by Afritech.

The nature, timing, and extent of testing conducted is considered sufficient and appropriate for the agreed scope of work, based on industry-recognised methodologies and the professional judgment applied to the associated risk. The results of this review should not be construed to imply any warranty over the functionality, quality, security or performance of the systems tested. Testing is a point-in-time assessment: Afritech reserves the right to amend this report if further vulnerabilities are subsequently detected by or reported to Afritech.

Confidentiality Notice

This document is proprietary to Afritech and contains confidential information of commercial value to Afritech, the disclosure of which to third parties could adversely affect the business affairs of Afritech.

This information is supplied in confidence to you, on the strict condition that no part of it is disclosed to any third party, in particular to any person or organization that may be in competition with Afritech without the prior written approval of Afritech.

Contents

General Information 5
Report Information 6
Approved Test House Information 6
Review Information 6
Security Dashboard 7
Executive Summary 8
Remediation Priority and Tracker 9
Attack Path Analysis 10
How Afritech Works With You 11
Summary of Scope 13
Summary of Testing Performed 15
Summary of Internal Network Security Assessment Findings 17
Details of Internal Network Security Assessment Findings 18
Finding 1: Domain Credentials Exposed in SYSVOL (Group Policy Preferences) 18
Finding 2: SMB Signing Not Required 19
Summary of External Network Security Assessment Findings 20
Details of External Network Security Assessment Findings 21
Finding 1: Apache Tomcat Remote Code Execution (CVE-2025-24813) 21
Finding 2: Weak TLS Protocols and Ciphers Enabled 22
Summary of Website Security Assessment Findings 23
Details of Website Security Assessment Findings 24
Finding 1: SQL Injection in Customer Search 24
Finding 2: Missing Brute-Force Protection on Login 25
Summary of Mobile Application Security Assessment Findings 25
Detail of Android Mobile Application Security Assessment Findings 27
Finding 1: Authentication Token Stored in Plaintext on the Device 27
Finding 2: Certificate Pinning Not Implemented 28
Detail of iOS Mobile Application Security Assessment Findings 29
Finding 1: Weak Jailbreak Detection 29
Finding 2: Sensitive Data Written to Application Logs 30

Summary of Firewall Security Assessment Findings 31
Detail of Firewall Security Assessment Findings 33
Finding 1: Any-Any Allow Rule From Internal Network to DMZ 33
Finding 2: Management Interface Reachable From Guest Wi-Fi 34
Summary of Firewall Vulnerability Assessment Findings 35
Detail of Firewall Security Vulnerability Assessment Findings 36
Finding 1: Outdated Firewall Firmware 36
Finding 2: SNMP v2c With Default Community String 37
Summary of Information Security Social Engineering Assessment 38
Phishing Campaign Results 39
Annexure A 40
Details of in-scope IP addresses that were tested 40
Annexure B 41
Details of the in-scope web addresses that were tested 41
Annexure C 42
Open ports and services identified for the in-scope internal IP addresses that were tested 42
Annexure D 43
Open ports and services identified for the in-scope external IP addresses that were tested 43
Annexure E 44
Details of the in-scope mobile applications that were tested 44
Annexure F 45
Firewall rules where findings were identified 45
In scope email addresses that were targeted 46
Affected Hosts Register 46

General Information

30 October 2026

THIRD-PARTY VULNERABILITY SCANNING AND PENETRATION TESTING REVIEW OF MERIDIAN PAYMENTS (PTY) LTD CONDUCTED DURING THE PERIOD 12 OCTOBER 2026 TO 23 OCTOBER 2026

Afritech has been appointed by Meridian Payments (Pty) Ltd to conduct third party vulnerability scanning and penetration testing, and to highlight any exceptions identified.

Afritech Computing (Pty) Ltd is an independent cyber security consulting company based in South Africa, specialising in vulnerability assessment and penetration testing.

The staff members involved in the vulnerability and penetration testing have IT auditing experience and have qualified as either Certified Information Systems Security Professionals ('CISSP') or Certified Ethical Hackers ('CEH'). As CISSP professionals, these individuals are required to utilize and comply with the International Information System Security Certification Consortium, (ISC)² Code of Professional Ethics to guide the professional and personal conduct of the members of the association. Certified Ethical Hackers are certified and governed by The International Council of E-Commerce Consultants.

Our enclosed report highlights our key findings as a result of the testing performed at Meridian Payments (Pty) Ltd during the period 12 October 2026 to 23 October 2026. Due to the nature of the environment, denial of service attempts and other tests that would have a high probability of causing disruption to the IT environment was excluded. Consequently, our findings may not include all possible weaknesses.

Afritech grants Meridian Payments (Pty) Ltd permission to disseminate this report for the purpose of disclosure within your organization. Distribution of this report will be pre-agreed with Afritech.

We would like to take this opportunity to thank the various members of your staff for their co-operation and assistance during the course of the testing. Please feel free to contact us at cybersecurity@afriteq.co.za should you have any questions or require further discussion.

Innocent Maluka
Director
Afritech Computing (Pty) Ltd

Client Information
Client Trading Name
Meridian Payments (Pty) Ltd

Report Information	
Report Number	**Report Date**
AFR-PEN-2026-014	30 October 2026

Approved Test House Information	
Name	**Address**
Afritech Computing (Pty) Ltd	Corporate Park North, 64 Roan Cres, Randjespark, Midrand, 1685, South Africa

Review Information		
Review Request Date	**Review Start Date**	**Review End Date**
28 September 2026	12 October 2026	23 October 2026

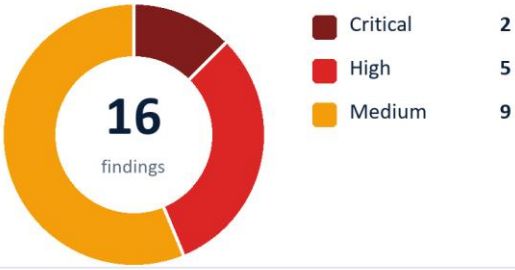
Employee Name	Experience	Certifications	Degrees
Innocent Maluka	13+ years of IT Security Assessments	Certified Ethical Hacker, Certified Penetration Testing Engineer, eLearn Mobile Application Penetration Tester, eLearn Junior Penetration Tester	-
Carl du Pisanie	4+ years of IT Security Assessments	Certified Ethical Hacker, Certified Penetration Testing Engineer, eLearn Junior Penetration Tester	-

Sample report: every name, address, IP address and finding in this document is fictional. It shows the structure, depth and plain-language guidance an Afritech client receives.

Security Dashboard

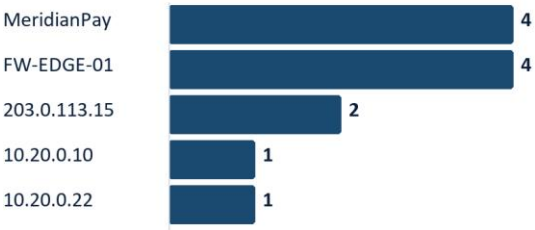
OVERALL RISK	FINDINGS	CRITICAL + HIGH	ASSETS AFFECTED
Critical	16	7	23

Findings by severity



Findings by area

Most affected assets



Highest-priority findings

- Critical — Apache Tomcat Remote Code Execution (CVE-2025-24813...
- Critical — Domain Credentials Exposed in SYSVOL (Group Policy Pref...
- High — Any-Any Allow Rule From Internal Network to DMZ (8.8)
- High — SQL Injection in Customer Search (8.1)
- High — Outdated Firewall Firmware (7.5)

Remediation plan

7	9	0
Fix first	**Fix next**	**Fix when convenient**
Critical and High: within 7 to 30 days	Medium: within 90 days	Low: within 180 days

Executive Summary

Overall risk rating: Critical

Afritech carried out a penetration test of Meridian Payments (Pty) Ltd's in-scope environment between 12 October 2026 and 23 October 2026. We identified 16 findings that need attention: 2 Critical, 5 High, 9 Medium and 0 Low. At least one Critical finding means an attacker could probably gain serious access with little effort. These need attention before anything else.

Area	Critical	High	Medium	Low	Total
Internal network	1	0	1	0	2
External network	1	0	1	0	2
Website / API	0	1	1	0	2
Mobile applications	0	1	3	0	4
Firewalls	0	2	2	0	4
Social engineering	0	1	1	0	2
Total	2	5	9	0	16

Findings to deal with first

- Apache Tomcat Remote Code Execution (CVE-2025-24813) (Critical, CVSS 9.8) - External network, 1 affected target
- Domain Credentials Exposed in SYSVOL (Group Policy Preferences) (Critical, CVSS 9.0) - Internal network, 1 affected target
- Any-Any Allow Rule From Internal Network to DMZ (High, CVSS 8.8) - Firewalls, 1 affected target

Recommended next steps

- Fix the Critical and High findings first. The Remediation Priority and Tracker section sets a target timeframe for each finding.
- Give each finding an owner and a target date in the tracker, and review progress regularly.
- Ask Afritech to retest once the fixes are in place, so the closure of each finding is confirmed rather than assumed.
- Repeat the assessment at least once a year and after major changes to the environment.

Remediation Priority and Tracker

Findings are listed in the order we recommend fixing them. The client completes the Owner and Date fixed columns and returns the table to Afritech with the retest request.

Priority	Finding	Area	Rating	Target	Owner	Date fixed
Fix first	Apache Tomcat Remote Code Execution (CVE-2025-24813)	External network	Critical	Within 7 days		
Fix first	Domain Credentials Exposed in SYSVOL (Group Policy Preferences)	Internal network	Critical	Within 7 days		
Fix first	Any-Any Allow Rule From Internal Network to DMZ	Firewalls	High	Within 30 days		
Fix first	SQL Injection in Customer Search	Website / API	High	Within 30 days		
Fix first	Outdated Firewall Firmware	Firewalls	High	Within 30 days		
Fix first	Authentication Token Stored in Plaintext on the Device	Mobile applications	High	Within 30 days		
Fix first	Phishing: meridianpay.example	Social engineering	High	Within 30 days		
Fix next	Management Interface Reachable From Guest Wi-Fi	Firewalls	Medium	Within 90 days		
Fix next	Weak TLS Protocols and Ciphers Enabled	External network	Medium	Within 90 days		
Fix next	Certificate Pinning Not Implemented	Mobile applications	Medium	Within 90 days		
Fix next	Sensitive Data Written to Application Logs	Mobile applications	Medium	Within 90 days		
Fix next	SMB Signing Not Required	Internal network	Medium	Within 90 days		
Fix next	Missing Brute-Force Protection on Login	Website / API	Medium	Within 90 days		
Fix next	SNMP v2c With Default Community String	Firewalls	Medium	Within 90 days		
Fix next	Weak Jailbreak Detection	Mobile applications	Medium	Within 90 days		
Fix next	Phishing: meridian-retail.example	Social engineering	Medium	Within 90 days		

Attack Path Analysis

Our assessment found two separate routes that each lead to the heart of Meridian Payments' environment, and they meet in the middle.

Route 1, from the internet: the internet-facing Tomcat server (203.0.113.15) accepts file uploads and allows an attacker to run their own code. From there the server can reach the internal network through the any-any firewall rule between the DMZ and the internal network.

Route 2, from a single staff member: in our phishing campaign 14 of 120 staff entered their password on a fake login page. With any one of those accounts, the administrator password recovered from SYSVOL works on 14 machines, and SMB relaying (signing is not required) extends that to the file servers.

How Afritech Works With You

Verified, not just scanned. Scanner output is the starting point. Our testers confirm each finding by hand, remove false alarms and show the evidence.

Plain-language results. Every finding explains what it means for your business, not just which setting is wrong, and says how to fix it.

A plan you can act on. The dashboard, executive summary and remediation tracker show what to fix first, by when, and let your team record progress.

Attack paths, not lists. We show how separate weaknesses combine, so you spend effort on the fixes that break real attack routes.

Retesting once you have fixed it. When your team has fixed the findings, we check that the fixes work and update the report.

Local, accountable people. Your assessment is led by named, certified South African testers (see the staff table), and you can reach them directly at cybersecurity@afriteq.co.za.

Either route ends with administrator control of the domain. Closing the seven items marked 'Fix first' in the remediation tracker breaks both routes.

Summary of Scope

The Internal Network Assessments aims to:

- Perform automated vulnerability scans using vulnerability scanning tools and interpret results to identify inherent flaws and control and/or configuration weaknesses in host technology directly supporting the Client's applications.
- Evaluate the visibility of the internal network i.e., intranet to potential threats.
- Determine if critical servers and workstations are adequately secured to prevent unauthorised access and limit internal malicious activity.
- Determine whether the internal network is configured according to best practices.
- Determine which protocols and services are active and accessible on each active port on the Client's internal network.
- Manually investigate host(s) vulnerabilities that cannot be identified or verified through automated means (including post exploitation and privilege escalation).

The External Network Assessments aims to:

- Identify inherent flaws, control and/or configuration weaknesses in the Client's external network.
- Perform automated vulnerability scans using vulnerability scanning tools and interpret results to identify inherent flaws and control and/or configuration weaknesses in the Client's external network.
- Determine which protocols and services are active and accessible on each active port on the Client's external network.
- Determine whether the external network is adequately secured to prevent unauthorised access and limit malicious activity by external users.
- Determine whether the external network is configured according to best practices.
- Determine whether the external network is securely configured and protected according to the most common vulnerability databases.
- Manually investigate host(s) vulnerabilities that cannot be identified or verified through automated means (including post exploitation and privilege escalation).

The Website Security Assessment aims to:

- Identify inherent flaws, control and/or configuration weaknesses in host technology directly supporting the Client's Internet-facing host.
- Determine whether the Internet-facing host is adequately secured to prevent unauthorised access and limit malicious activity by external users.
- Determine whether the Internet-facing host is configured according to best practices.
- Determine whether the Internet-facing host is securely configured and protected according to the most common vulnerability databases.
- Manually investigate host(s) vulnerabilities that cannot be identified or verified through automated means (including post exploitation and privilege escalation).

The Mobile Application Security Assessment aims to:

- Assess the security of Android mobile applications and devices to identify vulnerabilities and weaknesses that could be exploited by malicious actors.
- Collect information about the mobile application, including its functionality, purpose, and any available documentation.
- Identify the APIs, server endpoints, and communication channels used by the app.
- Understand the target device's operating system, version, and any relevant configurations.
- Evaluate the potential impact and likelihood of successful attacks based on the identified threats.
- Review the source code and binaries for potential vulnerabilities, using tools to identify common coding errors and security issues.

• Evaluate the effectiveness of authentication mechanisms and authorisation controls. • Attempt to exploit identified vulnerabilities to gain unauthorised access or control.
The Firewall Security & Vulnerability Assessment aims to
• Evaluate the rule configurations of the Client's firewall. • Perform automated vulnerability scans using vulnerability scanning tools to identify potential weaknesses in the Client's firewall configuration. • Determine the ability of firewall configurations to effectively permit authorized access and prevent unauthorised network access.
The Information Security Social Engineering Assessment aims to:
• Evaluate the users' awareness of social engineering threats. • Evaluate the ability of mail server configurations to prevent unauthorised access to critical data.
Anything not covered by the items outlined in the Scope of Work above will be considered out of scope.
Refer to Annexure A for the details of the in-scope IP addresses that were tested
Refer to Annexure B for details of the in-scope web addresses that were tested
Refer to Annexure C for the open ports and services identified for the in-scope internal IP addresses that were tested.
Refer to Annexure D for the open ports and services identified for the in-scope external IP addresses that were tested.
Refer to Annexure E for the details of the in-scope mobile applications that were tested.
Refer to Annexure F for the details of the firewall rules where findings were identified.
Refer to Annexure G for the details of the in-scope email addresses that were targeted.

Summary of Testing Performed

The review has been conducted using a best practice approach including a manual or automated Quality Assurance process of:

The Internal Network Assessment:

- Intelligence Gathering and Planning
- Threat Modelling
- Reconnaissance
- OS Identification
- Open Port Identification (1 to 65000 TCP and UDP)
- Vulnerability Scanning and Assessment
- Exploitation
- Lateral Movement and Pivoting
- Post-Exploitation Activities
- Data Exfiltration and Impact Testing
- Minimalizing of false positives, and
- Best practice vulnerabilities

The External Network Assessment:

- Intelligence Gathering and Planning
- Threat Modelling
- Reconnaissance
- OS Identification
- Open Port Identification (1 to 65000 TCP and UDP)
- Vulnerability Scanning and Assessment
- Exploitation
- Lateral Movement and Pivoting
- Post-Exploitation Activities
- Data Exfiltration and Impact Testing
- Minimalizing of false positives, and
- Best practice vulnerabilities

The Website Security Assessment:

- Reconnaissance
- Vulnerability identification
- Vulnerability exploitation
- Service Identification
- Authentication and Authorization Testing (A1 and A2)
- Sensitive Data Exposure Testing (A3)
- XML External Entity (XXE) Attacks (A4)
- Broken Access Control (A5)
- Security Misconfigurations (A6)
- Cross-Site Scripting (XSS) Attacks (A7)
- Insecure Deserialization (A8)
- Using Components with Known Vulnerabilities (A9)
- Insufficient Logging and Monitoring (A10)

• Minimalizing of false positives, and • Best practice vulnerabilities
The Mobile Application Security Assessment:
• Reconnaissance • Threat Modelling • Vulnerability Analysis • Authentication and Authorization Testing • Data Storage and Transmission Testing • Input Validation and Injection Testing • Session Management Testing • Cryptography and Key Management Testing • Code Review and Reverse Engineering • Android Platform-Specific Testing • Push Notification and Third-Party Integration Testing • Minimalizing of false positives, and • Best practice vulnerabilities
The Firewall Security & Vulnerability Assessments aims to:
• Evaluate the rule configurations of the Client's firewall. • Perform automated vulnerability scans using vulnerability scanning tools to identify potential weaknesses in the Client's firewall configuration. • Determine the ability of firewall configurations to effectively permit authorized access and prevent unauthorised network access.
The Information Security Social Engineering Assessment:
• Reconnaissance • Harvesting of email addresses publicly available on the Internet • Phishing campaign to assess user awareness and mail server configurations to prevent unauthorised access to critical data
Compliance with the relevant security requirements has been assessed using sufficient and appropriate testing procedures to ascertain compliance, and the approach tailored based on Afritech's cumulative audit knowledge and experience of the client.
Testing procedures included inquiry and discussion with key personnel, obtaining an understanding of the security environment, operational effectiveness of controls and compensating controls. Where findings were resolved during the review period, they were not included as part of this report.

Summary of Internal Network Security Assessment Findings

Vulnerability Severity Levels Based on the NVD and CVSS v3 Scoring System

Afritech has adopted the Common Vulnerability Scoring System (CVSS) version 3.1, an industry standard for the severity assessment of computer system security vulnerabilities. CVSS provides a way to capture the principal characteristics of a vulnerability, and produce a numerical score reflecting its severity, as well as a textual representation of that score.

The organization should take a risk-based approach to resolve or mitigate vulnerabilities identified in this report, starting with the most critical items and working down to the lower rated items. In order to obtain compliance, all vulnerabilities identified with risk ratings 4.0 through 10.0 should be managed/corrected to obtain an acceptable risk rating of less than rating 4.0. Vulnerabilities rated less than rating 4.0 are not included in this report.

Internal Network Security Assessment Findings Summary:

Rating category	The severity of findings based on NVD and CVSS combined base score	Number of findings identified
Critical	9.0 – 10.0	1
High	7.0 – 8.9	0
Medium	4.0 – 6.9	1
Low	0.1 – 3.9	0

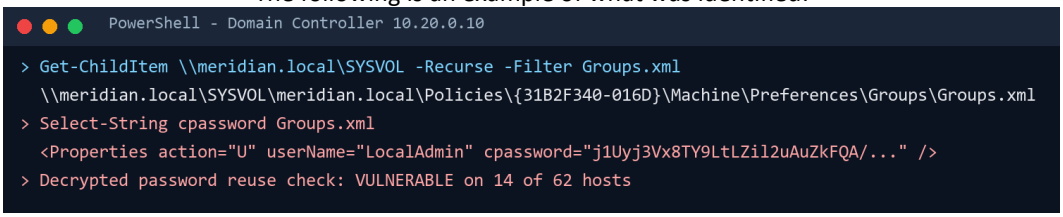
Details of Internal Network Security Assessment Findings

Finding 1: Domain Credentials Exposed in SYSVOL (Group Policy Preferences)

IP Address(es) (Port)	10.20.0.10(445/tcp)
CVSS Base Score	9.0
Rating	Critical
Remediation Priority	Fix first - within 7 days
Description	A Group Policy Preferences file in the SYSVOL share contains a 'cpassword' value for a local administrator account. Microsoft published the decryption key for this format in 2012, and every authenticated domain user can read SYSVOL. The recovered password was valid on 14 servers and workstations.
Business Impact	Any employee account, including a compromised one, could be turned into administrator access on most of the network within minutes. That is the usual route from a single phishing click to a full ransomware event.
What We Observed	10.20.0.10(445/tcp): Groups.xml under SYSVOL contains cpassword for user LocalAdmin. Decrypted value accepted by 14 of 62 hosts tested.
CVE Reference	No CVE reference Available
Suggested Solution	Delete the affected Group Policy Preferences items and rotate every password they contained. Deploy Windows LAPS so each machine has a unique, automatically rotated local administrator password.
Further Reading	https://support.microsoft.com/kb/2962486
Detected By / Retest	Manual verification (Group Policy Preferences audit). After the fix, Afritech re-runs this check on the affected targets to confirm it no longer appears.

Evidence

The following is an example of what was identified:



Finding 2: SMB Signing Not Required	
IP Address(es) (Port)	10.20.0.21(445/tcp) 10.20.0.22(445/tcp) 10.20.0.23(445/tcp) 10.20.0.24(445/tcp) 10.20.0.25(445/tcp) 10.20.0.26(445/tcp) 10.20.0.27(445/tcp) 10.20.0.28(445/tcp) 10.20.0.29(445/tcp) 10.20.0.30(445/tcp) ... and 4 more (full list in the Affected Hosts Register)
Targets Affected	14 targets
CVSS Base Score	5.3
Rating	Medium
Remediation Priority	Fix next - within 90 days
Description	These servers accept SMB connections without requiring message signing. An attacker on the network can relay captured authentication to them and act as the victim user.
Business Impact	Makes credential relay attacks possible. On its own it is a stepping stone, but it turns small footholds into access to file servers and applications.
What We Observed	10.20.0.21(445/tcp): SMB signing is enabled but not required on the remote host.
CVE Reference	No CVE reference Available
Suggested Solution	Set 'Microsoft network server: Digitally sign communications (always)' to Enabled through Group Policy for all servers and workstations, then confirm that no legacy system breaks.
Further Reading	https://learn.microsoft.com/windows-server/storage/file-server/smb-security
Detected By / Retest	Nessus plugin 57608. After the fix, Afritech re-runs this check on the affected targets to confirm it no longer appears.
Evidence	

The following is an example of what was identified:

```
nmap --script smb2-security-mode 10.20.0.21-34

$ nmap -p445 --script smb2-security-mode 10.20.0.21-34
PORT    STATE SERVICE
445/tcp open  microsoft-ds
| smb2-security-mode:
|   3.1.1:
|_    Message signing enabled but not required
```

Summary of External Network Security Assessment Findings

Vulnerability Severity Levels Based on the NVD and CVSS v3 Scoring System

Afritech has adopted the Common Vulnerability Scoring System (CVSS) version 3.1, an industry standard for the severity assessment of computer system security vulnerabilities. CVSS provides a way to capture the principal characteristics of a vulnerability, and produce a numerical score reflecting its severity, as well as a textual representation of that score.

The organization should take a risk-based approach to resolve or mitigate vulnerabilities identified in this report, starting with the most critical items and working down to the lower rated items. In order to obtain compliance, all vulnerabilities identified with risk ratings 4.0 through 10.0 should be managed/corrected to obtain an acceptable risk rating of less than rating 4.0. Vulnerabilities rated less than rating 4.0 are not included in this report.

External Network Security Assessment Findings Summary:

Rating category	The severity of findings based on NVD and CVSS combined base score	Number of findings identified
Critical	9.0 – 10.0	1
High	7.0 – 8.9	0
Medium	4.0 – 6.9	1
Low	0.1 – 3.9	0

Details of External Network Security Assessment Findings

Finding 1: Apache Tomcat Remote Code Execution (CVE-2025-24813)	
IP Address(es) (Port)	203.0.113.15(8080/tcp)
CVSS Base Score	9.8
Rating	Critical
Remediation Priority	Fix first - within 7 days
Description	The Tomcat 9.0.71 instance exposed to the internet is vulnerable to remote code execution through partial PUT requests when the default servlet is writable. Afritech confirmed that a harmless marker file could be written to the server. No further exploitation was performed.
Business Impact	An attacker anywhere in the world could run their own code on a server in your DMZ. This is the kind of flaw that automated attack tools exploit within days of publication.
What We Observed	203.0.113.15(8080/tcp): Server: Apache Tomcat/9.0.71 PUT of a marker file to the default servlet returned 201 Created.
CVE Reference	CVE-2025-24813
Suggested Solution	Upgrade Apache Tomcat to a fixed release (9.0.99 or later), disable write access on the default servlet, and remove the management interface from the internet.
Further Reading	https://tomcat.apache.org/security-9.html
Detected By / Retest	Apache Tomcat version detection and manual proof of write. After the fix, Afritech re-runs this check on the affected targets to confirm it no longer appears.
Evidence	

The following is an example of what was identified:

```
curl - 203.0.113.15:8080
$ curl -i http://203.0.113.15:8080/
HTTP/1.1 200
Server: Apache Tomcat/9.0.71
$ curl -X PUT http://203.0.113.15:8080/afritech-poc.session -d 'marker'
HTTP/1.1 201 Created        <- VULNERABLE: write accepted by default servlet
```

Finding 2: Weak TLS Protocols and Ciphers Enabled	
IP Address(es) (Port)	203.0.113.15(443/tcp) 203.0.113.20(443/tcp)
Targets Affected	2 targets
CVSS Base Score	5.9
Rating	Medium
Remediation Priority	Fix next - within 90 days
Description	Both servers still accept TLS 1.0 and TLS 1.1 and offer cipher suites that are considered weak.
Business Impact	Weak encryption puts payment and login traffic at risk of interception and can fail PCI DSS scans.
What We Observed	203.0.113.15(443/tcp): TLSv1.0 is offered TLSv1.1 is offered
CVE Reference	No CVE reference Available
Suggested Solution	Disable TLS 1.0 and 1.1 and weak cipher suites. Allow TLS 1.2 and 1.3 with modern AEAD ciphers only.
Further Reading	https://datatracker.ietf.org/doc/rfc8996/
Detected By / Retest	Nessus plugin 104743. After the fix, Afritech re-runs this check on the affected targets to confirm it no longer appears.
Evidence	

The following is an example of what was identified:

```
testssl.sh 203.0.113.15:443

$ testssl.sh --protocols 203.0.113.15:443
 SSLv3      not offered (OK)
 TLS 1      offered (deprecated)   <- NOT ok
 TLS 1.1    offered (deprecated)   <- NOT ok
 TLS 1.2    offered (OK)
 TLS 1.3    not offered
```

Summary of Website Security Assessment Findings

Vulnerability Severity Levels Based on the NVD and CVSS v3 Scoring System

Afritech has adopted the Common Vulnerability Scoring System (CVSS) version 3.1, an industry standard for the severity assessment of computer system security vulnerabilities. CVSS provides a way to capture the principal characteristics of a vulnerability, and produce a numerical score reflecting its severity, as well as a textual representation of that score.

The organization should take a risk-based approach to resolve or mitigate vulnerabilities identified in this report, starting with the most critical items and working down to the lower rated items. In order to obtain compliance, all vulnerabilities identified with risk ratings 4.0 through 10.0 should be managed/corrected to obtain an acceptable risk rating of less than rating 4.0. Vulnerabilities rated less than rating 4.0 are not included in this report.

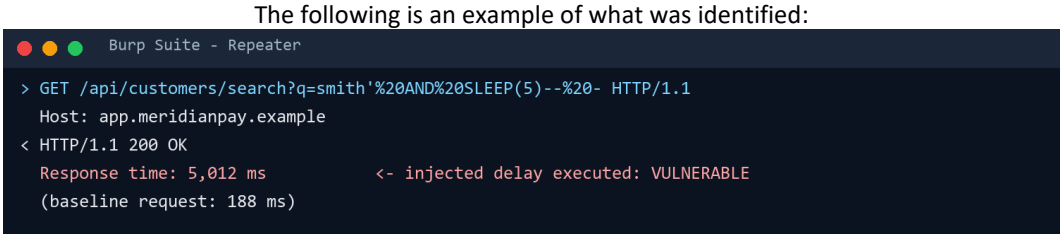
Website Security Assessment Findings Summary:

Rating category	The severity of findings based on NVD and CVSS combined base score	Number of findings identified
Critical	9.0 – 10.0	0
High	7.0 – 8.9	1
Medium	4.0 – 6.9	1
Low	0.1 – 3.9	0

Details of Website Security Assessment Findings

Finding 1: SQL Injection in Customer Search	
URL Address(es)	app.meridianpay.example
CVSS Base Score	8.1
Rating	High
Remediation Priority	Fix first - within 30 days
Description	The 'q' parameter of /api/customers/search is concatenated into a database query. An authenticated user could read records they should not see; the test stopped at proving the flaw with a harmless time-delay payload.
Business Impact	Customer and payment records could be read or changed by anyone with a login. This is reportable under POPIA and damaging to customer trust.
What We Observed	app.meridianpay.example: GET /api/customers/search?q=smith'+AND+SLEEP(5)--+- Response delayed by 5,012 ms (baseline 188 ms).
CVE Reference	No CVE reference Available
Weakness Class (CWE)	CWE-89
Suggested Solution	Use parameterised queries for all database access, validate input on the server and give the application's database account only the permissions it needs.
Further Reading	https://owasp.org/Top10/A03_2021-Injection/
Detected By / Retest	Burp Suite (confidence: Certain). After the fix, Afritech re-runs this check on the affected targets to confirm it no longer appears.
Evidence	

The following is an example of what was identified:



Finding 2: Missing Brute-Force Protection on Login	
URL Address(es)	portal.meridianpay.example
CVSS Base Score	5.3
Rating	Medium
Remediation Priority	Fix next - within 90 days
Description	The login endpoint accepts unlimited password attempts with no lockout, delay or CAPTCHA. 500 attempts were made in under a minute from a single address.
Business Impact	Attackers can test stolen passwords from other breaches against your customers' accounts until one works.
What We Observed	portal.meridianpay.example: POST /login, 500 attempts in 54 seconds, no lockout or rate limit observed.
CVE Reference	No CVE reference Available
Weakness Class (CWE)	CWE-307
Suggested Solution	Add rate limiting and temporary lockout, alert on repeated failures and offer multi-factor authentication.
Further Reading	https://owasp.org/Top10/A07_2021-Identification_and_Authentication_Failures/
Detected By / Retest	Burp Suite (confidence: Firm). After the fix, Afritech re-runs this check on the affected targets to confirm it no longer appears.

Evidence

The following is an example of what was identified:

```
Burp Suite - Intruder

> POST /login   (payload set: 500 passwords, 1 user)
  Attempts completed: 500 in 54 seconds
  Responses: 499 x 401 Unauthorized, 1 x 302 Found
  Lockout or rate limit observed: none          <- VULNERABLE
```

Summary of Mobile Application Security Assessment Findings

Vulnerability Severity Levels Based on the NVD and CVSS v3 Scoring System

Afritech has adopted the Common Vulnerability Scoring System (CVSS) version 3.1, an industry standard for the severity assessment of computer system security vulnerabilities. CVSS provides a way to capture the principal characteristics of a vulnerability, and produce a numerical score reflecting its severity, as well as a textual representation of that score.

The organization should take a risk-based approach to resolve or mitigate vulnerabilities identified in this report, starting with the most critical items and working down to the lower rated items. In order to obtain compliance, all vulnerabilities identified with risk ratings 4.0 through 10.0 should be managed/corrected to obtain an acceptable risk rating of less than rating 4.0. Vulnerabilities rated less than rating 4.0 are not included in this report.

Android Mobile Application Security Assessment Findings Summary:

Rating category	The severity of findings based on NVD and CVSS combined base score	Number of findings identified
Critical	9.0 – 10.0	0
High	7.0 – 8.9	1
Medium	4.0 – 6.9	1
Low	0.1 – 3.9	0

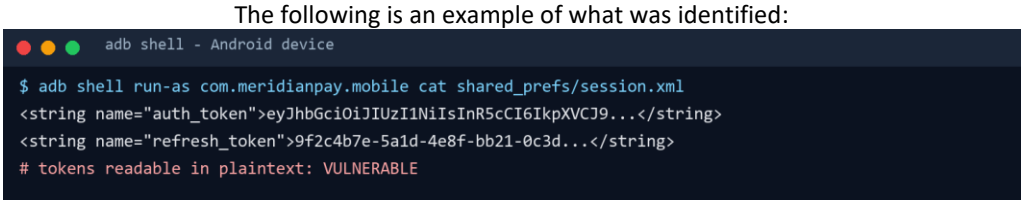
iOS Mobile Application Security Assessment Findings Summary:

Rating category	The severity of findings based on NVD and CVSS combined base score	Number of findings identified
Critical	9.0 – 10.0	0
High	7.0 – 8.9	0
Medium	4.0 – 6.9	2
Low	0.1 – 3.9	0

Detail of Android Mobile Application Security Assessment Findings

Finding 1: Authentication Token Stored in Plaintext on the Device	
Application	com.meridianpay.mobile 4.2.1 (Android 14)
Path(s)	/data/data/com.meridianpay.mobile/shared_prefs/session.xml
CVSS Base Score	7.1
Rating	High
Description	The app saves the customer's authentication and refresh tokens in an unencrypted preferences file. Anyone with physical access to an unlocked or rooted device, or a malicious app with backup access, can copy the tokens and use them from another device.
Reference	OWASP MASVS-STORAGE-1 / MASTG-TEST-0001
Suggested Solution	Store tokens in the Android Keystore (EncryptedSharedPreferences), keep their lifetime short and bind them to the device.
Evidence	

The following is an example of what was identified:



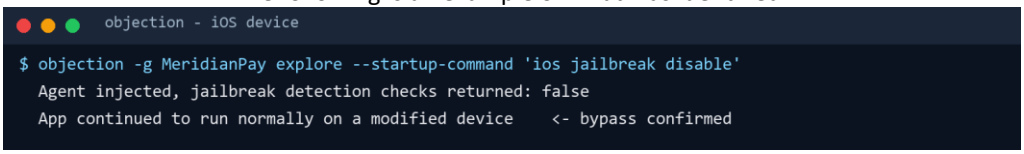
Finding 2: Certificate Pinning Not Implemented	
Application	com.meridianpay.mobile 4.2.1 (Android 14)
Path(s)	Network layer (OkHttp client)
CVSS Base Score	5.9
Rating	Medium
Description	The app trusts any certificate signed by a CA that the device trusts. A user on a hostile network can be tricked into installing a certificate, which lets an attacker read and change payment requests.
Reference	OWASP MASVS-NETWORK-2 / MASTG-TEST-0019
Suggested Solution	Pin the API certificate or public key, with a backup pin, and fail closed when validation fails.
Evidence	

The following is an example of what was identified:

Detail of iOS Mobile Application Security Assessment Findings

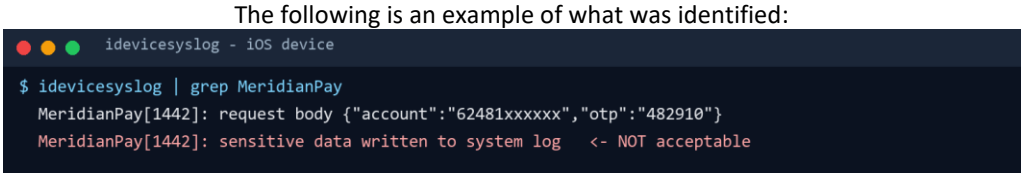
Finding 1: Weak Jailbreak Detection	
Application	MeridianPay 4.2.1 (iOS 17)
Path(s)	Runtime protections (ObjC/Swift)
CVSS Base Score	4.8
Rating	Medium
Description	The jailbreak check looks for a short list of file paths and can be bypassed with off-the-shelf tooling. The app continues to run, including payments, on a modified device.
Reference	OWASP MASVS-RESILIENCE-1 / MASTG-TEST-0048
Suggested Solution	Add layered integrity checks, treat a modified device as higher risk server-side and limit sensitive actions on it.
Evidence	

The following is an example of what was identified:



Finding 2: Sensitive Data Written to Application Logs	
Application	MeridianPay 4.2.1 (iOS 17)
Path(s)	Logging (os_log / NSLog)
CVSS Base Score	5.5
Rating	Medium
Description	Request bodies, including partial account numbers and one-time PINs, are written to the system log in the release build and can be read from a connected or backed-up device.
Reference	OWASP MASVS-STORAGE-2 / MASTG-TEST-0053
Suggested Solution	Remove sensitive values from logs in release builds and use a logging wrapper that redacts by default.
Evidence	

The following is an example of what was identified:



Summary of Firewall Security Assessment Findings

Vulnerability Severity Levels Based on the NVD and CVSS v3 Scoring System

Afritech has adopted the Common Vulnerability Scoring System (CVSS) version 3.1, an industry standard for the severity assessment of computer system security vulnerabilities. CVSS provides a way to capture the principal characteristics of a vulnerability, and produce a numerical score reflecting its severity, as well as a textual representation of that score.

The organization should take a risk-based approach to resolve or mitigate vulnerabilities identified in this report, starting with the most critical items and working down to the lower rated items. In order to obtain compliance, all vulnerabilities identified with risk ratings 4.0 through 10.0 should be managed/corrected to obtain an acceptable risk rating of less than rating 4.0. Vulnerabilities rated less than rating 4.0 are not included in this report.

The severity of Level Rating	Description
Critical	These issues can pose a very significant security threat. The issues that have a critical impact are typically those that would allow an attacker to gain full administrative access to the device. For a firewall device, allowing all traffic to pass through the device unfiltered would receive this rating as filtering traffic to protect other devices is the primary purpose of a firewall.
High	These issues pose a significant threat to security but have some limitations on the extent to which they can be abused. User-level access to a device and a DoS vulnerability in a critical service would fall into this category. A firewall device that allowed significant unfiltered access, such as allowing entire subnets through or not filtering in all directions, would fall into this category. A router that allows significant modification of its routing configuration would also fall into this category.
Medium	These issues have significant limitations on the direct impact they can cause. Typically, these issues would include significant information leakage issues, less significant DoS issues or those that provide significantly limited access. An SNMP service that is secured with default or a dictionary-based community string would typically fall into this rating, as would a firewall that allows unfiltered access to a range of services on a device.

Ease Rating	Description
Trivial	The issue requires little-to-no knowledge on behalf of an attacker and can be exploited using standard operating system tools. A firewall device that had a network filtering configuration that enables traffic to pass through would fall into this category.
Easy	The issue requires some knowledge for an attacker to exploit, which could be performed using standard operating system tools or tools downloaded from the Internet. An administrative service without or with a default password would fall into this category, as would a simple software vulnerability exploit.
Moderate	The issue requires specific knowledge on behalf of an attacker. The issue could be exploited using a combination of operating system tools or publicly available tools downloaded from the Internet.
Challenge	A security issue that falls into this category would require significant effort and knowledge on behalf of the attacker. The attacker may require specific physical access to resources or to the network infrastructure in order to successfully exploit the vulnerability. Furthermore, a combination of attacks may be required.
N/A	The issue is not directly exploitable. An issue such as enabling legacy protocols or unnecessary services would fall into this rating category.

Firewall Security Assessment Findings Summary:

Rating category	The severity of findings based on NVD and CVSS combined base score	Number of findings identified
Critical	9.0 – 10.0	0
High	7.0 – 8.9	1
Medium	4.0 – 6.9	1
Low	0.1 – 3.9	0

Detail of Firewall Security Assessment Findings

Finding 1: Any-Any Allow Rule From Internal Network to DMZ	
Device(s)	FW-EDGE-01
Ease Rating	Trivial
Rating	High
Description	A rule on FW-EDGE-01 allows all traffic from the internal network to every host in the DMZ, on every port. This was added as a temporary measure and never removed.
Impact	A compromised DMZ server, or any internal machine, can reach every service in both zones. Segmentation that should contain a breach does nothing.
Ease	Any internal user with basic tools can scan and connect to DMZ hosts without detection or restriction.
Suggested Solution	Replace the rule with explicit rules that name the sources, destinations and ports each service needs, then review quarterly.

Finding 2: Management Interface Reachable From Guest Wi-Fi	
Device(s)	FW-EDGE-01
Ease Rating	Easy
Rating	Medium
Description	The firewall's web and SSH management interfaces answer on the guest Wi-Fi network (VLAN 40).
Impact	Visitors and anyone who joins the guest network can attempt to log in to, or exploit, the device that protects the organisation.
Ease	Only needs a laptop on the guest Wi-Fi and a password-guessing or exploit tool.
Suggested Solution	Restrict management access to a dedicated management network or named administrator addresses, and require MFA.

Summary of Firewall Vulnerability Assessment Findings

Vulnerability Severity Levels Based on the NVD and CVSS v3 Scoring System

Afritech has adopted the Common Vulnerability Scoring System (CVSS) version 3.1, an industry standard for the severity assessment of computer system security vulnerabilities. CVSS provides a way to capture the principal characteristics of a vulnerability, and produce a numerical score reflecting its severity, as well as a textual representation of that score.

The organization should take a risk-based approach to resolve or mitigate vulnerabilities identified in this report, starting with the most critical items and working down to the lower rated items. In order to obtain compliance, all vulnerabilities identified with risk ratings 4.0 through 10.0 should be managed/corrected to obtain an acceptable risk rating of less than rating 4.0. Vulnerabilities rated less than rating 4.0 are not included in this report.

Firewall Vulnerability Assessment Findings Summary:

Rating category	The severity of findings based on NVD and CVSS combined base score	Number of findings identified
Critical	9.0 – 10.0	0
High	7.0 – 8.9	1
Medium	4.0 – 6.9	1
Low	0.1 – 3.9	0

Detail of Firewall Security Vulnerability Assessment Findings

Finding 1: Outdated Firewall Firmware	
Device(s)	FW-EDGE-01 (firmware 7.0.5)
CVSS Base Score	7.5
Rating	High
Description	The firewall runs a firmware release that the vendor no longer supports and that is affected by several published vulnerabilities, including remote code execution flaws in the management service.
CVE Reference	Multiple (see vendor security advisories for this release train)
Suggested Solution	Upgrade to the vendor's current supported firmware after taking a configuration backup, and subscribe to the vendor's security advisories.

Finding 2: SNMP v2c With Default Community String	
Device(s)	FW-EDGE-01 (UDP 161)
CVSS Base Score	5.3
Rating	Medium
Description	SNMP version 2c is enabled with the default community string 'public', which discloses the firewall's configuration, interfaces and routing table to anyone who can reach it.
CVE Reference	No CVE reference available
Suggested Solution	Disable SNMP, or move to SNMPv3 with authentication and encryption and restrict it to the monitoring server.

Summary of Information Security Social Engineering Assessment

Phishing Campaign
During the phishing attack, the target receives an email from IT Support stating that the target's email address has received multiple login attempts and is required to click on the link and report these attempts as being fraudulent. This email is disguised to be from a trusted source per domain (i.e., an address on the client's own domain) and contains a tracking link that opens an authentic looking webpage (i.e., Office365 clone website), and requires that the user logs into his/her Office365 account. Should the target fill out and submit the form, it would be used as evidencing for the effectiveness of employee awareness on phishing attacks.

Key	
Submitted form	The submit rate counts the number of distinct uses who have entered information into the webpage, possibly compromising their credentials which introduces a high risk of compromise
Clicked Link in email	The click-through rate counts the number of unique users who click the link in an e-mail, which introduces a medium risk of compromise. The link may take the user to a webpage that exploits client-side vulnerabilities to install malicious software on their computer without their knowledge.
Opened email	The e-mail open rate counts unique users who viewed the e-mail. The open rate is not a measure of risk, because opening an e-mail is very unlikely to compromise the user's machine.

Rating category	Total
High	1
Medium	1
Low/ None	0

Phishing Campaign Results			
Risk Rating	**Low/ None**	**Medium**	**High**
Domains Targeted	**Opened email**	**Clicked Link in email**	**Submitted form**
meridianpay.example (120 staff)	97 (81%)	41 (34%)	14 (12%)
meridian-retail.example (80 staff)	53 (66%)	17 (21%)	5 (6%)
Description	The click-through rate counts the number of unique users who click the link in an e-mail, which introduces a medium to high risk of compromise. The link may take the user to a webpage that exploits client-side vulnerabilities to install malicious software on their computer without their knowledge. The webpage may gather information on the user's browser and plug-ins, which the attacker can use to tailor an attack to known vulnerabilities. The submit rate counts the number of distinct uses who have entered information into the webpage, compromising their credentials. The e-mail open rate counts unique users who viewed the e-mail. The open rate is not a measure of risk, because opening an e-mail is very unlikely to compromise the user's machine. Still, an email open event confirms to the sender that the e-mail address is valid, which may invite future attacks. Open rates are measured by inserting a one-pixel image that is hosted on the instance into each e-mail. When a user opens an e-mail, the image is loaded. Because the image URLs for each email and user are unique, so it can be determined which users opened an email. However, because many e-mail clients do not load images by default to protect user privacy, the open rate often undercounts the number of users who have read the e-mail.		
Suggested Solution	To reduce the number of users that opens and responds on phishing attacks, it is recommended that a combination of security awareness training and technical controls.		

Annexure A

Details of in-scope IP addresses that were tested			
IP Address(es)			
10.20.0.10	10.20.0.21	10.20.0.22	10.20.0.23
10.20.0.24	10.20.0.25	10.20.0.26	10.20.0.27
10.20.0.28	10.20.0.29	10.20.0.30	10.20.0.31
10.20.0.32	10.20.0.33	10.20.0.34	10.20.0.50
10.20.0.51	10.20.0.52	203.0.113.10	203.0.113.15
203.0.113.20	203.0.113.25		

Annexure B

Details of the in-scope web addresses that were tested	
Web Address	**Services**
api.meridianpay.example	HTTP / HTTPS
app.meridianpay.example	HTTP / HTTPS
portal.meridianpay.example	HTTP / HTTPS
secure.meridianpay.example	HTTP / HTTPS

Annexure C

Open ports and services identified for the in-scope internal IP addresses that were tested

IP Address (Port/Protocol)		
10.20.0.10(53/tcp)	10.20.0.10(88/tcp)	10.20.0.10(135/tcp)
10.20.0.10(389/tcp)	10.20.0.10(445/tcp)	10.20.0.10(3389/tcp)
10.20.0.21(135/tcp)	10.20.0.21(445/tcp)	10.20.0.21(3389/tcp)
10.20.0.22(135/tcp)	10.20.0.22(445/tcp)	10.20.0.22(3389/tcp)
10.20.0.23(135/tcp)	10.20.0.23(445/tcp)	10.20.0.23(3389/tcp)
10.20.0.24(135/tcp)	10.20.0.24(445/tcp)	10.20.0.24(3389/tcp)
10.20.0.25(135/tcp)	10.20.0.25(445/tcp)	10.20.0.25(3389/tcp)
10.20.0.26(135/tcp)	10.20.0.26(445/tcp)	10.20.0.26(3389/tcp)
10.20.0.27(135/tcp)	10.20.0.27(445/tcp)	10.20.0.27(3389/tcp)
10.20.0.28(135/tcp)	10.20.0.28(445/tcp)	10.20.0.28(3389/tcp)
10.20.0.29(135/tcp)	10.20.0.29(445/tcp)	10.20.0.29(3389/tcp)
10.20.0.30(135/tcp)	10.20.0.30(445/tcp)	10.20.0.30(3389/tcp)
10.20.0.31(135/tcp)	10.20.0.31(445/tcp)	10.20.0.31(3389/tcp)
10.20.0.32(135/tcp)	10.20.0.32(445/tcp)	10.20.0.32(3389/tcp)
10.20.0.33(135/tcp)	10.20.0.33(445/tcp)	10.20.0.33(3389/tcp)
10.20.0.34(135/tcp)	10.20.0.34(445/tcp)	10.20.0.34(3389/tcp)
10.20.0.50(22/tcp)	10.20.0.50(80/tcp)	10.20.0.50(443/tcp)
10.20.0.51(1433/tcp)	10.20.0.51(3389/tcp)	10.20.0.52(445/tcp)
10.20.0.52(5985/tcp)		

Annexure D

Open ports and services identified for the in-scope external IP addresses that were tested		
IP Address (Port/Protocol)		
203.0.113.10(80/tcp)	203.0.113.10(443/tcp)	203.0.113.15(443/tcp)
203.0.113.15(8080/tcp)	203.0.113.20(443/tcp)	203.0.113.25(22/tcp)
203.0.113.25(443/tcp)		

Annexure E

Details of the in-scope mobile applications that were tested

Mobile Application	Package Kit File Name
MeridianPay Mobile (Android)	meridianpay-4.2.1.apk
MeridianPay Mobile (iOS)	MeridianPay-4.2.1.ipa

Annexure F

Firewall rules where findings were identified

Finding 1: Any-Any Allow Rule From Internal Network to DMZ								
FW-EDGE-01 - policy 'LAN-to-DMZ'								
Rule	**Active**	**Action**	**Protocol**	**Source**	**Src Port**	**Destination**	**Dst Port**	**Log**
14	Yes	Accept	ANY	LAN-10.20.0.0/24	ANY	DMZ-ALL	ANY	Disabled
15	Yes	Accept	TCP	LAN-10.20.0.0/24	ANY	DMZ-WEB	443	All

Finding 2: Management Interface Reachable From Guest Wi-Fi								
FW-EDGE-01 - policy 'GUEST-to-FW'								
Rule	**Active**	**Action**	**Protocol**	**Source**	**Src Port**	**Destination**	**Dst Port**	**Log**
31	Yes	Accept	TCP	GUEST-VLAN40	ANY	FW-MGMT	443, 22	Disabled

In scope email addresses that were targeted

Email address targeted	
finance@meridianpay.example	accounts@meridianpay.example
payments@meridianpay.example	hr@meridianpay.example
support@meridianpay.example	sales@meridianpay.example
it.helpdesk@meridianpay.example	operations@meridianpay.example

Affected Hosts Register

Findings that affect many targets list only the first few in the finding itself. The complete list for each is below.

Finding	Area	All affected targets
SMB Signing Not Required	Internal network	10.20.0.21(445/tcp) 10.20.0.22(445/tcp) 10.20.0.23(445/tcp) 10.20.0.24(445/tcp) 10.20.0.25(445/tcp) 10.20.0.26(445/tcp) 10.20.0.27(445/tcp) 10.20.0.28(445/tcp) 10.20.0.29(445/tcp) 10.20.0.30(445/tcp) 10.20.0.31(445/tcp) 10.20.0.32(445/tcp) 10.20.0.33(445/tcp) 10.20.0.34(445/tcp)