WeFuzz - Penzzer

NCSS ITSAR Security Test Report

Telecom FTP Server

Revision 1.0

NCSS ITSAR Security Test Report

Workspace:
Telecom FTP Server
Report Version:
v1.0
Date:
2025 - 4 - 28
Confidentiality:
Confidential

1. Executive Summary

- **Purpose:**

This NCCS ITSAR report was generated to evaluate the security posture of the product against the Indian Telecom Security Assurance Requirements (ITSAR).
It aims to verify compliance with mandatory security controls, identify potential vulnerabilities, and ensure that the product meets national cybersecurity standards prior to deployment in telecom networks.

- **Testing Scope:** FTP
  - **Compliance Summary:**
    * Total Requirements Evaluated: [X]
    * Fully Compliant: [ ]
    * Partially Compliant: [ ]
    * Non-Compliant: [X]

2. Introduction

- **Objective:**

The test objective, in the context of ITSAR, is to assess the product's adherence to the security requirements defined by the Indian Telecom Security Assurance Requirements (ITSAR) framework.
This involves systematically testing the product for vulnerabilities, verifying implementation of mandated security controls (such as access control, data protection, secure communication), and ensuring it meets the criteria for safe integration into national telecom infrastructure.
The goal is to validate the product's resilience against threats and its readiness for secure deployment.

- **Reference Documents:**
  * ITSAR Guidelines: v1.0.0
  * Product Technical Documentation - https://nccs.gov.in/home/itsars
  * RFCs / Standards (if any) - RFC 114, RFC 959, RFC 1123, RFC 2228, RFC 2389, RFC 2428, RFC 2577, RFC 3659, RFC 4217, RFC 5797

- **Test Environment:**
  * Location: Lab
  * Tools Used: Penzzer

* Duration: 1hours 20minutes 53seconds

- **Test Team:** We-Fuzz

3. System Description

- **System Components:**
  * FTP

4. ITSAR Compliance Mapping

Testing Area	Relevant Section(s)	FTP#Specific Test Cases
Robustness under invalid input	2.1, 2.2	Send malformed/truncated commands to test crash resistance
Buffer#overflow & long#argument handling	2.2	Use extremely long filenames, directory paths, or commands
Flood / DoS resilience	2.2, 2.3	High-rate ABOR/NOOP/ CDUP sequences + resource handling
Exception/resource management	2.3	Simulate memory/ cpu exhaustion, high concurrent sessions
Error logging during tests	2.4	Validate logs for commands that triggered exceptions

5. Test Methodology

- **Test Types:**
  * Dynamic Runtime Testing
  * Protocol Fuzzing
  * Configuration Review

- **Tools Used:** Penzzer
- **Test Plan Summary:**
  * Number of cases executed:
  * Protocols tested: FTP
  * Coverage achieved: 50.0%

6. Security Findings

Finding 1: **Overly long ABOR command**

- ITSAR Clause: NCCS ITSAR Clause 2.9.1 - "Fuzzing - Network and Application Level"

- Severity: High

- Description: The ABOR command is a standard part of the FTP protocol (RFC 959), used to abort a file transfer.

A "long ABOR command" represents an input anomaly — likely exceeding expected length or structure.

If this causes a crash, it indicates the system is not handling edge cases or malformed input safely.

Clause 2.9.1 The protocols supported by the CPE shall be robust when receiving unexpected or malformed inputs. This requirement shall be applicable for both network level as well as application-level protocols supported by the equipment.

- Test Performed: Overlong inputs

- Evidence: TCPv4 not arriving, expected to receive: ICMPv4, TCPv4 Last Packet(s) sent: ABOR 0x20 x 3,900

- Recommendation: Prevent the FTP service from crashing due to overly long ABOR command

- Status: Open

Finding 2: **Overly long CDUP command**

- ITSAR Clause: NCCS ITSAR Clause 2.9.1 - "Fuzzing - Network and Application Level"

- Severity: High

- Description: The CDUP command is a standard part of the FTP protocol (RFC 959), used to abort a file transfer.

A "long CDUP command" represents an input anomaly — likely exceeding expected length or structure.

If this causes a crash, it indicates the system is not handling edge cases or malformed input safely.

Clause 2.9.1 The protocols supported by the CPE shall be robust when receiving unexpected or malformed inputs. This requirement shall be applicable for both network level as well as application-level protocols supported by the equipment.

- Test Performed: Overlong inputs

- Evidence: TCPv4 not arriving, expected to receive: ICMPv4, TCPv4 Last Packet(s) sent: CDUP 0x20 x 1,100

- Recommendation: Prevent the FTP service from crashing due to overly long CDUP command

- Status: Open

7. Fuzz Testing Summary

- Tool: Penzzer
- Protocols Tested: FTP
- Test Coverage: 50.0%
- Crashes Detected: **Yes**
- Result: we have found 0 crashes

8. Remediation & Retesting

None

9. Conclusion

- Overall Result: **Non-Compliant**
- Deployment Recommendations: **Fix needed**
- Next Steps: **Further remediation**

End of Report