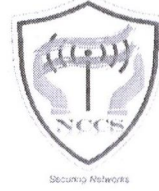




भारत सरकार  
संचार मंत्रालय  
दूरसंचार विभाग  
राष्ट्रीय संचार सुरक्षा केंद्र

Government of India  
Ministry of Communications  
Department of Telecommunications  
National Centre for Communication Security



Ltr No. NCCS/SAS/TSTP/2022-23/

dated at Bengaluru 1<sup>st</sup> January 2025

**Sub: List of 5G Network Function (Session Management Function - SMF) protocols which are to be subjected to fuzz testing**

1. The clause 2.9.1 of SMF ITSAR reads as follows:

“2.9.1 Fuzzing – Network and Application Level

Requirement:

It shall be ensured that externally reachable services of SMF are reasonably robust when receiving unexpected input.”

2. As per clause 2.3.6 of ITSAR, “SMF shall only run protocol handlers and services which are needed for its operation and which do not have any known security vulnerabilities. By default, all other ports and services will be permanently disabled. SMF Shall not support following services:”

FTP, TFTP, Telnet, SNMP v1 and v2, SSHv1, LLDP/CDP, HTTP, TCP/UDP Small Servers (Echo, Chargen, Discard and Daytime)”

Hence, no fuzzing test is required for these protocols

3. Based on the inputs received from different stakeholders during the meetings held with them, the list of protocols along with suggested suitable fuzz test are as detailed below.

**A. If only SMF Network Function (NF) is offered for testing by OEM:**

S NO	Name of the protocol	Suggested method of fuzz testing
1	PFCP (Packet Forwarding Control Protocol)	Generation based fuzzing
2	HTTPS (HTTP/2+TLS 1.2 and above)	Mutation based fuzzing
3	GTP-C (GPRS Tunneling Protocol - Control plane)	Generation based fuzzing
4	GTP-U (GPRS Tunneling Protocol - User plane)	Generation based fuzzing
5	SSHv2 and above	Generation based fuzzing
6	SNMPv3 and above	Generation based fuzzing

7	IPSec	Mutation based fuzzing
---	-------	------------------------

**B. If SMF Network Function (NF) along with cloud infrastructure like Kubernetes etc. is offered for testing by OEM:**

In addition to above mentioned seven protocols, the following protocols also shall be subjected to fuzz testing.

S NO	Name of the protocol	Suggested method of fuzz testing
1	IPv4	Mutation based fuzzing
2	IPv6	Mutation based fuzzing
3	ARP	Mutation based fuzzing
4	IPv6 ND	Mutation based fuzzing
5	TCP	Generation based fuzzing



Dir (SAS-III)

O/o Sr.DDG, NCCS, Bangalore