(24/C)

सत्यमेव जयते

भारत सरकार
संचार मंत्रालय
दूरसंचार विभाग
राष्ट्रीय संचार सुरक्षा केंद्र

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

Securing Networks

Ltr No. NCCS/SAS/TSTP/2022-23/20 dated at Bengaluru, 27th November, 2024

Sub: List of WiFi CPE protocols which are to be subjected to fuzz testing

1. The clause 9.1 of WiFi CPE ITSAR reads as follows:

   "9.1 Fuzzing – Network and Application Level

   Requirement:

   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.

   Note: Vendor is expected to provide the list of protocols supported by the Network product."

2. As per clause 3.6 of ITSAR, "by default the following services and their ports shall be initially configured to be disabled on the CPE by the vendor".

   FTP, TFTP, Telnet, SNMP V2, LLDP/CDP, HTTP"

   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 fuz test are as detailed below.

S NO	Name of the protocol	Suggested method of fuz testing
1	DHCP	Generation based fuzzing
2	ICMP	Generation based fuzzing
3	LWAPP	Mutation based fuzzing
4	CAPWAP	Mutation based fuzzing
5	NAT	Mutation based fuzzing
6	TLS 1.2 or higher	Mutation based fuzzing
7	UDP	Mutation based fuzzing
8	TCP	Generation based fuzzing
9	HTTPS	Mutation based fuzzing
10	WPA2	Generation based fuzzing
11	WPA3	Generation based fuzzing
12	ARP	Mutation based fuzzing

27/11/24.

Dir (SAS-III)
O/o Sr.DDG, NCCS, Bangalore