I/3088308/2023

Ministry of Communications
Department of Telecommunications
Networks & Technologies (NT) Wing

Dated: 02.03.2023

Office Memorandum

Subject: Advisory Guidelines to M2M/IoT stakeholders for securing consumer IoT

1. IoT is one of the fastest emerging technology across the globe which is being used to create smart infrastructure in various verticals such as Power Sector, Automotive, Safety & Surveillance, Remote Health Management, Agriculture, Smart Homes, Smart Cities etc using connected devices. M2M/IoT eco-system is proliferating very rapidly and being facilitated by recent advances in several technologies such as sensors, communication technologies (Cellular and non-cellular), AI/ ML, Cloud computing, Edge computing etc.
2. It has been projected that there would be around 11.4 billion consumer IoT devices and 13.3 billion enterprise IoT devices globally by 2025 i.e. consumer IoT devices would account for nearly 45% of all IoT devices.
3. In view of the anticipated growth of M2M/IoT devices, it is important to ensure that the M2M/IoT end-points comply with the safety and security standards and guidelines in order to protect the users and the networks that connect these devices. Hacking of the devices/networks being used in daily life would cause significant harm. Therefore, securing the M2M/IoT eco-system end-to-end i.e. from devices to the applications is very important.
4. Based on the TEC Technical Report "*Code of Practice for securing Internet of Things (IoT)*", the following broad guidelines are hereby issued to all M2M/IoT stakeholders :

A. **No universal default passwords**

i. Many M2M/IoT devices are being sold with universal default usernames and passwords (such as 'admin, admin') and this has been the source of many security issues in these devices which needs to be eliminated. Thus, all such device default passwords shall be unique per device and/or require the user to choose a password that follows best practices, during device provisioning. The passwords must not be resettable to any universal default value.
ii. Best practices on passwords and other authentication methods shall be followed such as the use of the strongest possible password appropriate to the usage context of the device.
iii. Associated web services shall use Multi-Factor Authentication and shall not expose any unnecessary user information prior to authentication.
iv. Any password reset process shall be possible only after appropriate authenticating of the user.

B. **Implement a means to manage reports of vulnerabilities**

i. M2M/IoT stakeholders shall provide a dedicated public point of contact as part of a vulnerability disclosure policy for security researchers and others to report security issues.
ii. Disclosed vulnerabilities shall be acted on in a timely manner by M2M/IoT stakeholders.
iii. The cyber security community shall be encouraged and rewarded for

I/3088308/2023

identifying and reporting vulnerabilities, thereby facilitating the responsible and coordinated disclosure and remediation of vulnerabilities.

C. **Keep software updated**

i. Software components in M2M/IoT devices shall be securely updateable. Updates shall be timely and shall not adversely impact the functioning of the device.
ii. An end-of-life policy shall be published for end-point devices which explicitly states the assured duration for which a device will receive software updates. For constrained devices that cannot physically be updated, the product shall be isolatable and replaceable.
iii. The retailer and/or manufacturers shall inform the consumer in a timely manner that an update is required and the need for each update(s) shall be made clear to consumers.
iv. An update shall be easy to implement, preferably using non-intrusive approaches like over the air (OTA) updates.
v. Regular software updates shall be provided after the sale of a device and pushed to devices for the lifecycle of the device. This period of software update support shall be made clear to a consumer when purchasing the product.
vi. If a user interface is available, it shall clearly display when a device has reached its end-of-life, inform the user of the risk of security updates no longer being available and provide suggestions for mitigating this risk.

This is issued with the approval of competent authority.

Signed by Ajay Nain
Date: 02-03-2023 12:09:27
Reason: Approved

(Ajay Nain)
ADG (NT-III),DoT HQ
Minto Road, New Delhi

To:

1. All M2M Service Providers

Copy to:

1. All Telecom Service Providers
2. DGT-HQ,for kind info.please.
3. Sr. DDG(TEC),for kind info. please.
4. DDG (Security),DoT HQ
5. ADG(IT), for uploading on DoT website