D-Link International Pte Ltd

IMDA TS RG-SEC Request for Comment

To

Aileen Chia (Ms)
Deputy Chief Executive (Policy, Regulation & Competition Development)
Director-General (Telecoms & Post)
Infocomm Media Development Authority
10 Pasir Panjang Road
#03-01 Mapletree Business City
Singapore 117438

Company: D-Link International Pte Ltd

Address: 1 International Business Park, Synergy #03-12 Singapore 609917

Name: Jonathan Quek

Title: Product Director (Consumer)

Email: jquek@sg.dlink.com

Contact: 66229365

D-Link International Pte Ltd

Question 1: IMDA invites comments relating to the requirements on preloaded credentials and password strength for RGs as set out in paragraph 4.1.

D-Link:

When user first purchase the product, our wizard will guide user for setup and enforce them to input the GUI administration password

Pre-loaded Credentials and password: Will have concern in the situation where rework of the on hand stock as unique password will not able to do a mass rework and need to rework by per units

Please note that Google website certificate do not allow https to be redirect and might have issue if enforce redirect to our Router GUI

If we can more "standard" with other country, it will be easier in term of economy of scale and effort on firmware development

NIST guidelines

In June 2017, the United States National Institute of Standards and Technology (NIST) issued a new revision of their digital authentication guidelines, NIST SP 800-63B-3, stating that:[13]:5.1.1.2

- Passwords must be at least 8 characters in length if chosen by the subscriber.

Minimum password strength:

Possible to be done but concern that user will forget the password easily and need to reset the router to recover which will result in lose of the configuration and setting, it will be tedious for "layman" to set up the router again

Question 2: IMDA invites comments relating to the requirements on preloaded settings for RGs as set out in paragraph 4.2.1.

D-Link:

WPS enable is important especially for MESH solution for quick pair up, previously security concern is mainly on the WPS-PIN rather than the physical WPS operation

HNAP is use for our APP communication with devices on the set up and control, our HNAP only contain basic information without any sensitive content. Before the launch of our wireless product, it will need to pass through the "Third Party" security lab to clear before introducing to the market

Firewall need to turn on by default as firewall sometime might slow down the performance. NAT default will able do basic block from WAN to LAN

These tunnel (Teredo, 6to4 etc) are mainly created from the OS, blocking might create unexpected issue or affect certain function of the OS. Microsoft request for IOT, gaming console like **X-BOX Live** request to support TEREDO

https://support-origin.xbox.com/th-TH/xbox-on-windows/social/troubleshoot-party-chat
https://support-origin.xbox.com/en-PH/xbox-on-windows/social/server-connectivity-xbox-app-displays-blocked

4.2.2 Initial setup Handling

D-link

Support WPA/WPA2 setup, depend on the wireless client use, it will use WPA2 as first choice unless client cannot support WPA2 (Older clients) than it will fall to WPA

4.2.3 Authentication handling

D-Link

After 5-time unsuccessful login, it will delay for 60 sec before user can attempt again.

Any advise on alternate authentication as we do not keep user information on the router, it is hard to provide alternate login option

D-Link International Pte Ltd

Question 4: IMDA seeks feedback on the feasibility for RG to be updated automatically with the latest firmware as outlined in paragraph 4.3. IMDA welcomes suggestions on possible implementation of automatic updates of RG's firmware, including the management of disrupted update processes.

D-Link

4.3. a Need user approval/Enable for automatic FOTA, we did not enforce automatic FOTA by default due to some cases, user do not want to be upgrade firmware automatically especially if they are using for certain project

Some device has dual image, which will maintain previous firmware if newer firmware upgrade was interrupted accidentally while writing flash. However, some device don't have this, so user will need to manually recover the device. Normally firmware will update estimated 0200hr – 0400hr (GMT 8)

Question 5: While IMDA does not specify any timeline for security patches to be made available upon the finding of new vulnerabilities, IMDA seeks views on the typical duration for patches to be made available, and whether there is a need to impose such a timeline for patches to be applied.

D-Link: Depend on the security issue severity and the party involved, e.g Chipset base code. Typically within 2 months to provide solution, for urgent case may take 1~2 weeks , case by case basis

Question 6: IMDA seeks comments on the requirements on the protection measures set out in paragraphs 4.4 to 4.5, in particular the requirement to display warning(s) of the higher security risk should weaker encryption algorithms be chosen

D-Link: Same concern as Section 4.1.2 as stated above

Our default is WPA/WPA2, WPA2 is priority if client able to support. No WEP supported

Data is encrypted as for 4.5 (b), it will be case by case basis

Question 7: IMDA seeks feedback on the requirement for RG to validate data inputs via all interfaces as outlined in paragraph 4.6. IMDA also seeks feedback on the possible documents/information to be submitted for IMDA verification of this requirement when performing equipment registration.

D-Link, we will be certified by IEC 62443-4-1 which cover the 4.6

Question 8: IMDA seeks views on what standards or guidelines are being used by RG manufacturers in developing their vulnerability disclosure policies.

D-Link: IEC 62443-4-1 and new router is verified by 3 party security check

END