McAfee’s response to IMDA Security requirements for Residential Gateways

Authors:

- Benny Chee
- Chan Lee
- Shashwat Khandelwal
- Vibhu Rishi

Contact information:

Benny Chee

Head of APAC Partner Product Management, McAfee

benny_chee@mcafee.com

+65 9833 1153

Shashwat Khandelwal

Head of Southeast Asia Consumer Business, McAfee

shashwat_khandelwal@mcafee.com

+65 9109 5027

McAfee Singapore Address:

238A Thomson Road,
#12-01/05, Novena Square
Tower A, Singapore 307684

Contents

Summary 3

Statement of Interest 4

Comments 5

Conclusion 8

Summary

This document covers McAfee’s response to the IMDA request for comments for the Security Requirements for Residential Gateways.

Statement of Interest

McAfee has been working with router manufacturers for the last few years to increase the security capabilities with recent threats which target user's home networks. These threats can range from sleeper botnets as seen in the case of the DynDNS DDOS attack or malware on routers. This is exacerbated by the fact that routers have minimal to no security in place. We bring to the table our wide experience in fighting against such cyber threats.

The McAfee approach is router agnostic as we run as a service on routers. The service is capable of scanning the devices in the network and detects unauthorized control within the network and alerts the home users for any such anomalies. McAfee software running on the router communicates with the McAfee Global Threat intelligence to protect against existing and new threats.

Comments

Security Requirements for Residential Gateways

References:

- Document 1 - Consultation document (603.85KB)
- Document 2 - IMDA TS RG-SEC document (650.89KB)

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

Each router at a minimum should have a different default password. This can be printed on the bottom of the box for user reference. McAfee recommends that the preloaded credentials be mandatory to set by the user on first login. Further the router manufacturer can provide a simple flag or an API to help in knowing whether the password has been changed or not. The password strength as laid down in the document is as per industry standards and should be adhered to.

It is also recommended that the user interface be developed which is easy enough for non-technical users to be able to interact with ease. Onboarding for the users should be via a mobile app so that it becomes easier for the user to access the router functionalities.

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

McAfee agrees to these recommendations. Security by default should be the mantra and one way of achieving it is to turn off modules by default which are not required by most people.

Question 3: IMDA seeks feedback on the requirements on RG administration as set out in paragraph 4.2, in particular the applicability of maintaining secure communication protocols such as SSH or HTTPS for device management interfaces to the RG as indicated in paragraph 4.2.5.

McAfee agrees that communication channels should be protected via secure protocols like SSH / HTTPs.Protocols like telnet should be disabled by default.

McAfee recommends remote administration via a secure channel from a trusted authorized device or app. The remote administration must only communicate through a secure cloud and all remote administration endpoints should also communicate through the cloud for any administration changes to the RG. There is no direct communication between the RG and the admin device or app. In this manner the admin can control the RG and the services running on the RG remotely and securely from anywhere.

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.

One of the major attack vectors are old vulnerabilities which do not get patched. Routers are inherently at risk as they never get updated. It is highly recommended that routers get updated on a regular basis with security patches. In case the router has old firmware or outdated modules, the user should be notified. Further it is suggested that the router have capabilities to updates each module separately.

It is also suggested that it be specified for how long the manufacturer will support the updates for each router model.

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.

McAfee recommends that patches should be updated automatically by the router manufacturer as soon as possible, and not later than 1 month after the vulnerability has been found.

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.

It is common practice to educate the less technically savvy users on the implications of having lower levels of security. An example is the prompt for strengthening the password by using various combinations and notifying the user whether his password is weak or strong. Similarly, the routers should display visually to the users the repercussion of using weaker encryption standards.

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.

It is recommended that the router interfaces be hardened against common attack vectors. McAfee recommends that only authorized devices or apps be able to access the router admin interfaces through a secure cloud interface and no other device or app in the network be able to access the admin functionalities.

RG manufacturers should also get the routers penetration testing done by 3rd parties. This can then be used for the overall score of the security of the routers.

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

McAfee is aligned with IMDA guidelines on disclosure policies.

Question 9: IMDA welcomes suggestions on other possible recommendations to secure the RGs.

Possible recommendations from McAfee:

- One of the threats users face is a rogue entity joining the user’s network (wifi hi-jacking) and then using the network to carry out attacks. This can be drastically reduced if the user is intimated (via app) for any new device which joins the WiFi network, as that will let a user know if the device which joined is expected or unknown.

- Not just the router, but most iot devices are currently at a very low level of security. These devices can get malware on them and start to cause unforeseen issues like a DDOS. Its recommended that routers have capabilities to detect rogue transmissions from such devices.

Question 10: IMDA invites comments on the proposed implementation plan and timelines.

McAfee solutions to secure the routers is already in the market in many geos like Americas, LTAM, EMEA. We have our services running with companies like Verizon, Telefonica.

Question 11: IMDA invites comments on the proposed equipment registration process for RGs

McAfee is aligned with IMDA guidelines on this.

Conclusion

We feel that the direction that IMDA is taking with respect to the security requirements for residential gateways is the right one. It is the need of the hour to make sure that the basic infrastructure that the world depends on for connectivity, especially in such times, should be made secure against cyber threats. It is also required that these security aspects be treated as a matter of policy as the average individual is not well versed with how to secure the gadgets. As such, it falls on the RG manufacturers and security devices to make their devices as robust as possible.

We believe that security should be by default and not an afterthought. The consideration of security is more than just the router device - it is the entire connected ecosystem in the home which has to be secured. As such, when we think of home security, we should be looking at each aspect of the WiFi security, from RG to all the connected devices.

A possible weak link to the security is the user themselves. This is primarily due to the lack of education and well as not having a security orientated mindset for the average person. A step in the direction is the security score for every router will enable the user to make informed choices. Another important aspect is easy user experience for connecting and accessing the router functionality. Capabilities like being able to know which devices joined the network, which devices are acting abnormally, which devices are using default password – will all go towards making our home networks much more secure.