LINKSYS RESPONSE TO

DOCUMENT 1

CONSULTATION PAPER ISSUED BY THE
INFO-COMMUNICATIONS MEDIA DEVELOPMENT AUTHORITY

SECURITY REQUIREMENTS FOR RESIDENTIAL GATEWAYS

10 April 2020

Proposed Security Requirements for Residential Gateways

Login Credentials (Ref: IMDA TS RG-SEC Paragraph 4.1)

4. Many of the RGs today come pre-loaded with default login credentials, such as usernames and passwords, for access to the RGs' administration page[1]. These factory pre-loaded default login credentials are often weak, not unique and almost never require any changes throughout their use, and hence can be easily compromised by actors and perpetrators, to gain and take control of the RGs for malicious cyber activities. IMDA TS RG-SEC will thus require that these factory pre-loaded login credentials be randomised and unique for each RG, with minimum password strength as specified. If factory pre-loaded default login credentials are provisioned, users will be required to change these credentials before the RGs can be used.

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

[1] RG's administration page allows the RG's configurations and settings to be changed.

Linksys Response to Question 1: For Linksys, user experience and easy to setup product is our core product value and priority. RG will not be functional until the setup wizard is completed. In the setup process itself, we will enforce our user to change the default password according to minimum password strength requirement.

Device Setup & Administration (Ref: IMDA TS RG-SEC Paragraph 4.2)

5. With technology advancements, RGs today come with many additional features and functions. An example would be Universal Plug and Play (UPnP), which allows devices connected to the RG to seamlessly discover each other's presence and establish functional network services for data sharing. Although such features and functions could be useful, they also provide openings for cybersecurity attacks if users are unaware that they have been activated. Considering that many users do not use these functions, the IMDA TS RG-SEC will require that these interfaces be turned off by default. In addition, the IMDA TS RG-SEC will also require the preloaded settings of RGs to disable some protocols/mechanisms that could be exploited, such as Home Network Administration Protocol (HNAP) and IPv6 tunnelling.

6. In addition to having secure preloaded settings for RGs, it is also important for RGs to be set up properly, such as ensuring that only authorised personnel can configure them. Hence, the IMDA TS RG-SEC will specify the handling of authentication and passwords. The IMDA TS RG-SEC will also require the device management interface to be secure, thereby preventing communication channels from being sniffed by unauthorised actors.

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

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.

Linksys Response to Question 2: Most of the protocol mentioned is not enabled in our product (HNAP, SNMP, NAT-PMP, Telnet, Transitional IPv6 tunnelling implementation).

We also do not enabled direct Remote Administration on WAN interface. Alternative way to remote manage the router is provided via secured cloud platform.

We also would like to highlight to IMDA that some of the protocol mentioned is essential for the home network to function and for compliance:

- WPS is required to be enabled by default as it is still an industry standard for connection method that are used by customers and Wi-Fi devices (i.e. printers). WPS is also part of Wi-Fi Alliance certification compliance.
- UPnP does not exist on WAN interface. We need to keep UPnP (LAN facing) enabled in order for common application in the home network to run (e.g. social messaging apps & gaming console)

Linksys Response to Question 3: SSH protocol is not enabled in our product. Enabling HTTPS in our product by default may impact on the users experience when they try to access the local management UI and create confusion to them. The security warning page may hinder users to continue to use the product, which is what we want to avoid. Users has the option to enable HTTPS from the local management UI. Considering IMDA's recommendation to implement a security certificate inside the RG's platform, may increase cost per units.

Firmware Updates (Ref: IMDA TS RG-SEC Paragraph 4.3)

7. The updating of the RGs' firmware with latest security patches is just as critical as any of the above mentioned security measures. Frequent timely updates will help to ensure that the RGs are protected against newer threats or newly found security lapses. However, it is noted that users may not update their RGs' firmware, even if security patches have been made available, thus making the RGs vulnerable. Hence, the IMDA TS RG-SEC will require the RGs to download and update the latest available firmware versions automatically. Nonetheless, IMDA is mindful that if the updating of firmware is disrupted or not done properly, it could affect the RGs' proper functioning subsequently. Thus, the IMDA TS RG- SEC does not specify the minimum period for the RG to be updated with the latest firmware.

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.

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.

Linksys Response to Question 4: Automatic Firmware Upgrade feature is already enabled by default in all of our product as long as users are following the proposed setup procedure (i.e. Setup wizard, or Mobile App). Auto Firmware Update checking occurs every midnight router's local time daily. In this case, the router will check for newer firmware availability via secured HTTPS communication and update automatically whenever available. All the new firmware posted on the Update Server are going through a very stringent QA processes to ensure minimum disturbance to end users normal network operation.

To avoid disturbance during the firmware upgrade process, RG will have two NVRAM partitions to store the firmware. The firmware upgrade process (i.e. download, store, and install) will happen on second partition, while the main partition is to keep current firmware version. If the update process is interrupted (e.g. power supply tripped), RG may still use the main partition to load the current firmware.

Linksys Response to Question 5: The duration of the security fix will vary depends entirely on the complexity of the solution, the severity level and the impact to the end users. Internal cross-functional team not limited to hardware, firmware, software, cloud, QA, Customer Support, chipset availability, etc, should be taken into consideration as well. Linksys have dedicated security team and ready to response with regards in handling the security vulnerability concern whenever it arises. The approach taken can either be a firmware update, security advisory or mitigation steps in which will be shared via security advisory page.

Wireless Access & Data Protection (Ref: IMDA TS RG-SEC Paragraphs 4.4 & 4.5)

8. In addition to securing the access to the RG and having updated firmware, the RG should also ensure that its communication with connected devices in the home is secure. The IMDA TS RG-SEC will specify default encryption algorithms for such communications and the storage of data that they use. The RG shall also allow the user to set up guest networks with separate login credentials for authorised guest users of the home network.

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.

Linksys Response to Question 6: The router default security encryption for wireless is AES with WPA2 Personal as default wireless protection. WEP protection may no longer be supported in the future.

Guest Network is available for users to configure to provide access to guest users. The guest network is separated from main network via different SSID and VLAN and it is isolated from the main network.

Encrypting the information used and stored by the router may increase the additional time to process such information to display and store from the router. Such delay may not be acceptable to the end users.

Validation of Data Inputs (Ref: IMDA TS RG-SEC Paragraphs 4.6)

9. IMDA notes that RGs will remain vulnerable if the data inputs are executed without being validated, exposing attached devices to known security vulnerabilities, such as Information leakage, remote code execution and cross- site scripting. The IMDA TS RG-SEC will thus require the RG to validate data inputs via all interfaces.

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.

Linksys Response to Question 7: The effort required for the RG to go through every single ingress scenario and ensure there is no information leakage, remote code execution, and cross-site scripting would be extreme large and time consuming. This would cause a huge noticeable delay/ performance degradation and it may not be acceptable to the end users.

We rely on internal and external testing as well as a public vulnerability disclosure program to ensure that we are testing our validations as much as possible.

Vulnerabilities Reporting (Ref: IMDA TS RG-SEC Paragraphs 4.7)

10. IMDA notes that it is not uncommon for new vulnerabilities of RGs to be discovered by various research institutes, organisations and individuals over time. Hence, IMDA views that it is important for RG manufactures to provide contacts for the public to inform them of the discovered vulnerabilities, allowing the manufacturers to develop security patches to address these vulnerabilities. In addition, IMDA understands that RG manufacturers would typically establish vulnerability disclosure policies.

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

Linksys Response to Question 8: Public security, safety and privacy are paramount. Decisions regarding when and how to execute public disclosure of vulnerabilities are made in the interest of best protecting consumers from exploitation of any vulnerability.

Approaches to public disclosure must be carefully considered. Publication of a previously unknown vulnerability prior to its resolution educates malicious parties and provides them a window of opportunity to exploit said vulnerability. This could encourage malicious activity and increase risk to consumers. For this reason, parties in the consumer networking industry such as Belkin and Security Researchers commonly adhere to coordinated disclosure principles, typified by The CERT® Guide to Coordinated Vulnerability Disclosure
(https://resources.sei.cmu.edu/asset_files/SpecialReport/2017_003_001_503340.pdf)

Under the principle of coordinated vulnerability disclosure:

- Security Researchers disclose newly discovered vulnerabilities to Belkin privately; to a national CERT or other coordinator who will report to Belkin privately; or to a private service that will report to Belkin privately;
- The Security Researcher will provide Belkin the opportunity to diagnose and offer fully tested updates, workarounds, or other corrective measures before any party discloses detailed vulnerability or exploit information to the public;
- PSIRT will coordinate with the Security Researcher throughout the vulnerability investigation and provide the Security Researcher with updates on case progress;
- Coordinated public disclosure most often will be made upon release of the vulnerability resolution, subject to various exceptions described in this policy;

In the event that the vulnerability is or becomes actively exploited prior to vulnerability's resolution, both the Security Researcher and Belkin will work together as closely as possible to provide early public vulnerability disclosure to protect customers.

To report any vulnerability discovered, researcher/reporter may visit Belkin coordinated public vulnerability disclosure program at this webpage:
https://www.belkin.com/us/security/
Release information on the appropriate Belkin/Linksys security advisory webpages:
https://www.linksys.com/us/support-article?articleNum=246427

Other Recommendations

11. The industry concerned should assess the impact of the proposed security requirements on RGs registered with IMDA, to be deployed on broadband networks in Singapore.

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

Linksys Response to Question 9: NA

Implementation Plan and Timelines

12. Following the close of the consultation, IMDA will review and assess all responses received prior to finalising the IMDA TS RG-SEC. The finalised IMDA TS RG-SEC will be in force 6 months from its publication date. IMDA considers that a 6-month duration will be sufficient for suppliers to bring in new RGs or refresh existing RGs to comply with the security requirements stipulated in the new IMDA TS RG-SEC.

13. Concurrently, IMDA plans to require the cessation of the sale of any previously registered RGs, which are not in compliance with IMDA TS RG-SEC, 1-year from the publication date of the IMDA TS RG-SEC. The timelines with the key milestones are shown in the attached **Annex A**.

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

Linksys Response to Question 10: We will follow the target implementation as stated in IMDA's Document 1 page 9.

Proposed Registration Scheme and process for RG

14. Today, equipment suppliers seeking to import and sell RGs are required to register the RG with IMDA by making an online declaration of conformity to the IMDA TS SRD[2] via the Enhanced Simplified Equipment Registration (ESER)[3]. Once the device is successfully registered with IMDA it can be released for sale for local use. Following the publication of the finalised IMDA TS RG-SEC, registations for RGs can be submited via a fresh registration under the ESER by making the necessary online declaration of conformity to IMDA TS RG-SEC and IMDA TS SRD for the RG models, and with the relevant supporting documents.

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

[2] IMDA Technical Specifications for Short Range Devices

[3] ESER is a self-declaration scheme where approval can be based on a declaration of conformity that does not need prior verification by IMDA. No registration fee is required.

Linksys Response to Question 11: Understand once RG-SEC is published, we can do the registration online like we are doing for SRD in ESER. We suggest there should be a professional team or labs available by IMDA for Linksys to make enquiry or to test and ensure our products are complied with the requirements.

And for the online registration, other than the checklist/supplier's declaration of conformity in Annex A, Linksys would like to have a clear instruction of the relevant supporting documents that we have to submit along with online registration.