LINKSYS RESPONSE TO

DOCUMENT 2

TECHNICAL SPECIFICATION

SECURITY REQUIREMENTS FOR RESIDENTIAL GATEWAYS

10 April 2020

Conformance Testing / Verification Checklist

This Checklist is intended for facilitating Supplier's Declaration of Conformity to the technical requirements defined in the IMDA Technical Requirements for Security Requirements for Residential Gateways ("IMDA TS RG-SEC")

P lease note:

"**CR**" indicates that the technical requirement set out in a particular section or sub-section ("§") of the IMDA TS RG-SEC is a **Compliance Requirement**.

"**M**" means that it shall be **Mandatory** for the Residential Gateways to comply with the technical requirement set out in the IMDA TS RG-SEC § cited in this Checklist (Table given below).

"**C**" means that compliance with the technical requirement set out in the IMDA TS RG-SEC § cited in this Checklist is **Conditional**. In this case, the need to comply is contingent on the conditions as indicated in the remarks column.

"**V**" means that compliance with the requirement is **Voluntary**.

IMDA TS RG-SEC §	Parameter	Description	CR	Yes/No/NA	Linksys Comments	Remarks
4.1	Login Credentials Management	The Residential Gateway with default login credentials, such as usernames and passwords, can be easily compromised, thereby allowing an attacker to gain access and use the device for malicious activities such as participation in botnets to perform DDoS attacks, Man-in-the-Middle attacks and/or through it to infiltrate other connected home IoT devices. The following measures are typical of industry practices to ensure that login credentials used for access controls are adequately protected.	-	-		
4.1.1	Factory pre-loaded Login Credentials	Factory pre-loaded login credentials such as passwords shall be randomised and unique for each Residential Gateway. If default login credentials are used, the Residential Gateways shall be in a disabled state (non-functioning) until the user successfully set new login credentials upon first attempt to	M	Yes	Residential Gateway is in non-functioning state before setup. Users will be required to complete the setup before the RG is in functional state. During the setup, users will be enforced to follow the minimum password strength.	

		access the device’s administration login page and the device’s configuration settings.				
4.1.2	Minimum Password Strength	Access to Residential Gateway’s administrative login page and device’s configuration settings shall only accept unique passwords that meet the following requirements:				
	4.1.2.a	The minimum length of a password shall be 10, and shall meet at least 3 out of the following 4 complexity rules: i. Minimally 1 uppercase character (A-Z) ii. Minimally 1 lowercase character (a-z) iii. Minimally 1 digit (0-9) iv. Minimally 1 special character (punctuation and/or space)	M	Yes		
	4.1.2.b	The password shall not have consecutive identical characters.	M	Yes		
	4.1.2.c	Values used in the login ID and password shall not be the same.	M	Yes		
4.2	Device Setup & Administration	The Residential Gateway needs to manage and control the access to device’s administration page; ensuring only authorised personnel are able to edit the configuration settings. While it is important to restrict intruder access, the Residential Gateway also needs to protect the device from being unintentionally or maliciously locked out.	-	-		

4.2.1	Device Pre-loaded Settings		-	-		
	4.2.1.a	The Residential Gateway shall turn off the following system services by default: i. WPS ii. HNAP	C	No	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. Our router does not support HNAP.	If the features are available in the Residential Gateway
	4.2.1.b	The Residential Gateway shall turn off the following Residential Gateway WAN interfaces by default: i. Remote Administration ii. SNMP iii. NAT-PMP iv. Telnet v. UPnP	C	Yes	SNMP, NAT-PMP & Telnet are not enabled on our product. Direct Remote Administration is not enabled on **WAN interface**. Alternative way to remote manage the router is provided via secured cloud platform (see 4.2.3.e). UPnP does not exist on **WAN interface** either. 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)	If the features are available in the Residential Gateway
	4.2.1.c	The Residential Gateway shall disable feature(s) that collects and sends the device's network statistics data back to manufacturer by default.	C	N/A	Such feature does not exist	If the features are available in

						the Residential Gateway
	4.2.1.d	The Residential Gateway shall turn on its firewall by default and support NAT to prevent its internal systems from being accessed directly from the Internet.	C	Yes	For IPv4 NAT will be enabled by default	If the features are available in the Residential Gateway
	4.2.1.e	The Residential Gateway shall disable IPv6 tunnelling mechanisms by default. Most modern operating systems use IPv6 by default and thus, some operating systems will attempt to pass IPv6 traffic in an IPv4 wrapper using tunnelling capabilities, such as Teredo, 6to4, or ISATAP. These tunnels could be used to create a hidden channel of communication to and from the Residential Gateway.	C	Yes	Transitional IPv6 implementation (e.g. Toredo, 6to4, or ISATAP) is not enabled on our product.	If the features are available in the Residential Gateway
4.2.2	Initial Setup Handling	First attempt to access to the Residential Gateway's administration page/settings should be conducted through a wired connection. If a wireless connection is used, the wireless communication should leverage on at least AES encryption, with at least WPA2 protection.	V	Yes	Device default security out of the box is AES encryption.	
4.2.3	Authentication Handling	The Residential Gateway shall ensure strong authentication, and protect against brute force and/or other abusive login attempts to the administration page/settings [ENISA GP-TM-25]:	-	-		

	4.2.3.a	Unprotected access to the Residential Gateway's management webpage shall be prohibited.	M	No	Access to management webpage can only be done locally when connected to the network physically, either wired or wireless. First layer of security has already in place for wired (you need to be physically connected with UTP cable attached) and wireless (WPA2 PSK with AES encryption) Users has the option to enable HTTPS from the local management UI.	
	4.2.3.b	Authentication credentials shall be salted, hashed and/or encrypted. [ENISA GP-TM-24].	M	Yes		
	4.2.3.c	Incremental prolong periods of login delay shall be employed after each subsequent failed attempt.	M	Yes		
	4.2.3.d	The login account shall be blocked after a fixed number of unsuccessful login attempts.	M	Yes		
	4.2.3.e	Secure alternative authentication mechanism shall be provided to fall-back on, when a login account is blocked. [GSMA CLP.13]	M	Yes	Secured Cloud login is available for customers that have signed up with Linksys Smart Wi-Fi account.	
4.2.4	Credentials Handling	The Residential Gateway shall ensure that the credentials are properly managed to avoid them being compromised when they are used:	-	-		
	4.2.4.a	Password fields shall prevent its contents from being copied.	M	Yes		

	4.2.4.b	Password shall never be displayed on a user’s screen and shall always be masked with the asterisk character, or another benign glyph. [GSMA CLP.13]	M	Yes		
	4.2.4.c	Password recovery or reset mechanism shall be protected and does not supply an attacker with any form of information indicating a valid account [ENISA GP-TM-26]	M	Yes	Our products has password recovery/reset mechanism guide from GUI that can only be accessed physically. Alternatively, users can factory reset their unit and reconfigure the new password.	
	4.2.4.d	Network management credentials, e.g., remote login credentials specified in Broadband Forum’s Technical Report 069 (“TR-069”) 1 , shall not be displayed on the Residential Gateway’s management web page.	M	Yes		
4.2.5	Device Management Interface	The Device management interface to the Residential Gateway shall be protected via secure communication protocol such as SSH or HTTPS to prevent the communication channel from being sniffed by unauthorised actors with malicious intent. Signed certificates from a Certification Authority (“CA”) and self-signed certificates can be considered for this purpose.	M	No	SSH is not enabled on 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.	
4.3	Firmware Updates		-	-		
	4.3.a	The Residential Gateway shall automatically download the latest security patches.	M	Yes		

	4.3.b	The Residential Gateway shall be updated with the latest security patches automatically. Patching could be carried out through different means and mechanisms, e.g., when Residential Gateway is powered off and on.	M	Yes	By default, the auto Firmware update option is enabled when a user follows the setup wizard. Auto Firmware Update checking occurs every midnight router's local time daily. In this case, the router will check for newer FW availability via secured HTTPS server and update automatically.	
	4.3.c	The Residential Gateway should also provide means for users to manually run and install the downloaded security patches.	V	Yes	End user has the option to disable the auto Firmware update. They can download the FW from Linksys website and have an option to manually upgrade to the router firmware via GUI.	
	4.3.d	The Residential Gateway shall verify the patches are digitally signed before installing them.	M	No	digital signing of images is undesirable with GPLv3 license. In any cases, our firmware is tested and verified through stringent QA process before releasing it to public to ensure a very minimum impact to end users. We also use a secured HTTPS server for firmware update services via cloud.	
	4.3.e	Minimum period of the firmware support received by the Residential Gateway shall be provided upfront to the user.	M	Yes		
	4.3.f	The device manufacturer should ensure the patches: i. do not contain sensitive data such as	V	Yes		

		hardcoded credentials; and ii. are transmitted via secured connection.				
	4.3.g	Security updates for the Residential Gateway should be provided in a timely manner. "Timely" in this context varies with the criticality of the identified vulnerability, the availability of a fix and the complexity of fix. The complexity of the fix is dependent on factors, such as constrained devices, involvement of multiple stakeholders, hardware versus software fix, etc.	V	Yes		
4.4	Wireless Access Protection		-	-		
	4.4.a	The Residential Gateway should employ strong passwords as described in Section 4.1.2 for Wi-Fi connection.	V	Yes		
	4.4.b	The Residential Gateway shall use AES encryption, with at least WPA2 protection by default. If weaker security protection such as WEP or WPA is chosen by users, warning(s) of the higher security risk to use these encryption algorithms shall be displayed.	M	Yes		
	4.4.c	The Residential Gateway shall allow and recommend to the user to setup guest networks with separate passwords for authorised guest users & guest IoT devices of the home network, isolating these accounts from the main home network.	M	Yes		

4.5	Data Protection		-	-		
	4.5.a	The Residential Gateway shall encrypt the data elements that it uses and stores with standardised encryption algorithms (e.g., AES) with no known vulnerability.	M	No		
	4.5.b	Encryption algorithms used should be replaceable so that improved encryption algorithms can be adopted without significant change to existing device.	V	No		
4.6	Validation of Data Inputs	Data input to the device via all interfaces shall be validated, to protect the Residential Gateway from actions such as information leakage, remote code execution and cross-site scripting.	M	No	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.	
4.7	Vulnerabilities Reporting	A point of contact, e.g., email address and contact number shall be provided to allow the reporting of security vulnerabilities relating to the Residential Gateway.	M	Yes	Linksys do have a coordinated public vulnerability disclosure program to submit any vulnerability found by third party pen-tester here: https://www.belkin.com/us/security/	