Response to Invitation to Comment

Cisco Systems

CONSULTATION PAPER ISSUED BY THE INFO-COMMUNICATIONS MEDIA DEVELOPMENT AUTHORITY - SECURITY REQUIREMENTS FOR RESIDENTIAL GATEWAYS

Company Overview

Cisco (www.cisco.com) is the worldwide leader in IT that helps companies seize the opportunities of tomorrow by proving that amazing things can happen when you connect the previously unconnected.

At Cisco customers come first and an integral part of our DNA is creating long-lasting customer partnerships and working with them to identify their needs and provide solutions that support their success.

The concept of solutions being driven to address specific customer challenges has been with Cisco since its inception. Husband and wife Len Bosack and Sandy Lerner, both working for Stanford University, wanted to email each other from their respective offices located in different buildings but were unable to due to technological shortcomings. A technology had to be invented to deal with disparate local area protocols; and as a result of solving their challenge - the multi-protocol router was born.

Since then Cisco has shaped the future of the Internet by creating unprecedented value and opportunity for our customers, employees, investors and ecosystem partners and has become the worldwide leader in networking - transforming how people connect, communicate and collaborate.

Point of Contact

Joshua McCloud, National Cybersecurity Officer

Cisco Security & Trust Organization

Cisco Systems, Inc.

Email: jmccloud@cisco.com

Telephone: +65 9638 9289

Table of Contents

Statement of Interest

Cisco, as a vendor, is a provider of commercial network infrastructure, collaboration, and security products and services. The contents of this submission does not make any direct references to such products and services, but are our observations and recommendations.

Question 1

IMDA invites comments relating to the requirements on pre-loaded credentials and password strength for Residential Gateways (RGs) as set out in paragraph 4.1.

- Reference 4.1: Multi-factor authentication (MFA) is fast becoming a critical capability where users interact with services. This should be encouraged as a more secure means of authentication after the initial setup. In addition to forcing the selection of a username / password, we also suggest (or mandate) supporting MFA.
- Reference 4.1: Password requirements are a little light. For example "Pas$word123" would be permitted under the current draft. Passwords authentication should be consistent with NIST SP 800-63 Authenticator Assurance Level 1 or above and meet the criteria under section "5.1.1.2 Memorized Secret Verifiers" of NIST SP 800-63B on Digital Identity Guidelines. NIST shows that complexity requirements can be counterproductive. It is more important to compare passwords against a 'blacklist' of unacceptable passwords (e.g. "password").
- Reference 4.1: The maximum password length should be stipulated at 64 characters.

Question 2

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

- Reference 4.2.1: The default state for the RG should be as secure as possible with features not necessary to the basic functioning of the device disabled by default. In addition to disabling remote administration, SNMP, NAT-PMP, Telnet, UPnP on WAN interfaces, these services should also be disabled for LAN or local interfaces by default.
- Reference 4.2.1: NAT should be enabled by default, not just supported.
- Reference 4.2.1: Users should be required to change the default SSID.

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.

- Reference to 4.2: We disagree on providing consumer guidance that the first attempt at setup should be conducted through wired ports. Ethernet ports in home devices, laptops, etc. are becoming rare. Whether wired or wireless-based setup, appropriate security should be used. Instead, initial setup guidance for the consumer could state that connecting to an Ethernet port to conduct initial setup is recommended if possible, otherwise, the consumer should follow the best

practice for initial setup over wireless. We agree that initial setup over wireless should only be conducted with WPA2 and AES at a minimum.

- Reference 4.2.3: It is Important that any locking delay invoked only applies to the admin page and does not impact the actual gateway functionality of the device or other functionality such as media server, etc. Otherwise, this may create a denial-of-service by malware or remote attackers deliberately failing password attempts.
- Reference 4.2.4 d: The introduction to this specification says it is for devices to be "… better protected when purchased and deployed by consumers, thus safeguarding both the Communications Network and the home IoT devices …" If RA is positioned as a consumer device that is not expected to be managed by a service provider, it is not clear why is there is TR-069 capability at all. For the RA category of devices, we suggest that there should not be an open port 7547 to even connect, let alone reveal a password to.
- Reference 4.2.5: SSH and HTTPS should be disabled on the WAN interface and only HTTPS with at least TLS 1.2 or greater should be enabled on local interfaces. SSH should be disabled by default for all interfaces.

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.

- Reference 4.3 a, b, c: These requirements could have some order of preference, minimally with the default of firmware auto-downloaded and auto-applied / restart during the night. As part of the initial setup configuration, the user can be given the option to change the time period for updates or, as a last resort, choose to manually update. Additionally, some indication of a need to upgrade could come from the RG (e.g. LED, splash page on adminstratvie GUI). However, these options are not reliable as most users will not monitor the RG once it is setup.
- Reference 4.3 d: In addition to the RG verifying that the patches are digitally signed, the patches should be cryptographically validated and, if invalid, the upgrade process should halt. This guidance should be made clearer.
- For disrupted updates, the RAs should automatically detect the failure and roll-back to the current version before attempting to upgrade again. If updates continue to fail, an LED warning light and/or splash page on the administrative GUI can notify the user of the upgrade failure with instructions for contacting vendor technical support.

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.

- Cisco can provide the following reference:

- https://tools.cisco.com/security/center/resources/vendor_vulnerability_policy.html

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.

- Reference 4.4 and 4.5: We agree with the recommendation. Warning messages should discourage users from selecting weaker encryption algorithms and possibly include a brief explanation (e.g. these older, weaker algorithms are susceptible to compromise that may enable an attacker to steal your data or hack into your network).

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.

- Reference 4.6: Validating input is essential and should require specific secure coding techniques be followed (e.g. the OWASP Top 10). This section needs to be strengthened and provide clearer guidance. Vendors should be required to furnish evidence of secure software development practices that include baseline policies that their developers must follow and appropriate static testing results. Below are key validation requirements that can be considered where applicable:
    - Protect command processors from injection vulnerabilities by preventing the execution of arbitrary commands or code.
    - Protect against SQL injections by using primary defences when the program builds an SQL statement.
    - Protect against URL injections by applying input validation and structured URL practices when using URLs or generating URLs from user-supplied data.
    - Validate all input before processing it (e.g. buffer input length validation, character type validation).
    - Protect against XML entity injection vulnerabilities by disabling entity expansion or validating text content after expansion.
    - Protect against XPATH Injection vulnerabilities using prepared statements or validating user input to construct XPath queries.
    - Protect against NoSQL injection attacks by validating user-supplied input before the program builds a NoSQL database query.

Question 8

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

- Cisco can provide the following references to our vulnerability disclosure policies:
    - https://tools.cisco.com/security/center/resources/security_vulnerability_policy.html
    - https://tools.cisco.com/security/center/resources/vendor_vulnerability_policy.html

Question 9

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

- Offer secure DNS services: We recommend considering providing the user with an option to select the use of a "Secure DNS" provider during initial device setup and configuration.
- Encourage trustworthy platforms: We recommend considering a requirement for vendor trustworthy compliance. Key components of demonstrating “trustworthiness” can include:
    - Demonstrated supply chain security program;
    - Demonstrated Secure Development Lifecycle program;
    - Demonstrated strong internal security practices (i.e. InfoSec/SecOps);
    - Implementation of secure boot technologies (e.g. TPM chips, cryptographically signed software);
    - Use of OS runtime defences (e.g. object size checking, ASLR, etc).
- Securely store credentials and sensitive data: Passwords, credentials and encryption keys, as well as personally identifiable, or financial information must be treated as sensitive data and protected accordingly. Secure storage should also be defined. TPM chips are examples of hardware mechanisms for storing keys and other information that can then be used to encrypt and securely store sensitive data. While such hardware mechanisms are important, not all devices will be able to achieve this. There should also be consideration for features for the simple and effective removal of all data from a device and/or associated services. For consumers, this minimizes potential data loss when disposing or RGs.
- Ensure that personal privacy data is protected: Consumer privacy is of key concern. Seeking consent should be separate from any other user acceptance and should be positive consent requiring user action.
- Streamline consumer premises equipment: Having separate ONT and consumer gear may be necessary for now, but it is a poor use of resources in the medium to longer term. The reason for the split is so that service providers can deliver a consistent service

without consumer interference, while giving consumers a choice in terms of the quality and capability of their devices.

What IMDA should focus on in the medium term are strong standards for ONT connectivity (e.g. DOCSIS) that will provide for a choice of the ONT device for performance and technology enablement. Consumers tend to have little interest in manageability or understanding of security, even if they have a preference for the speed or bandwidth of the devices and their specific feature set such as Wi-Fi 6, mesh capability, etc. It is better that security aspects be addressed with higher level service offerings. It should be required that these offerings be made part and parcel of provisioning broadband service.

- Prioritize home IoT security as a national security consideration: We offer the following scenario regarding how IoT vulnerabilities can impact national security:

  Consider a consumer oven that connects back to its manufacturer and provides an app to see what is going on. Each of these devices has a thermostat, a heating element, a fan, and a control interface that consists of a display and some knobs and buttons that are all linked to a PLC/CPU and some firmware and memory. There is also a transceiver.

  The device speaks to the cloud so that the user can view its state in an app. But the moment a device has a CPU and transceiver with software or firmware, there is a risk of defects and vulnerabilities. Often, the only question is whether those defects or vulnerabilities have been discovered by a hacker. We must assume that the answer is yes because that is often the case. All it takes is a copy of the firmware and it can be disassembled to identify known vulnerabilities.

  So now the hacker has access to the oven. That means the hacker can control the oven; turning it on, setting the temperature, turning it off. The hacker can use the oven to attack other devices, either in the consumer's home or elsewhere as Mirai demonstrated when DVRs were used to attack Dyn's name servers and took Twitter offline.

  Now assume that the oven is a common model. The hacker could indiscriminately, or with the help of a geolocation database in a targeted fashion, turn on a group of ovens all at once; perhaps a large group. Perhaps 20-30 thousand. Maybe the attack has also been used to attack the thermostat. So now the hacker could turn on the air-conditioner as well. If we consider the resulting power draw on a neighbourhood or within a city, this could lead to outages or worse.

  We can say the oven manufacturer should always automatically install the latest firmware and should have a path for communication of bugs. But realistically the hacker will be faster. How do we protect that oven and how do we protect the infrastructure?

  That is the argument for micro-segmentation in the home. A service provider needs to manage this because the consumer simply cannot.

Question 10

IMDA invites comments on the proposed implementation plan and timelines.

- No comment

Question 11

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

- No comment

Annex – References

- NIST SP 800-63B: https://pages.nist.gov/800-63-3/sp800-63b.html
- CIS Internet Controls: https://www.cisecurity.org/newsletter/10-tips-to-securely-configure-your-new-devices/
- OWASP Top Ten: https://owasp.org/www-project-top-ten/