California Senate Bill 327

This technical note provides information about the new California law, Senate Bill 327, as follows:

1. Highlights what you can expect from this Bill in 2020 in our PDU products and firmware.
2. Informs you of Raritan's action plan and implementation strategy for compliance.
3. Tells you what to do if you perform automated or bulk configuration/provisioning of new PDUs.

What Is This Bill?

Senate Bill 327 is a cybersecurity law covering Internet of Things (IoT) devices that requires minimum security features for every device.

Starting January 1, 2020, SB-327 requires any manufacturer of a device that connects "directly or indirectly" to the internet to be more responsible for ensuring privacy and security for California residents by equipping devices with "reasonable" security features that are designed to prevent unauthorized access, modification, or information disclosure.

If the device can be accessed outside a local area network with a password:

1. The device needs either to come with a unique password for each device, or
2. The device must force users to set their own password the first time they connect, eliminating generic default credentials that could be hacked. **Note: This is the route Raritan has chosen to implement.**

A "connected device" is defined as a device with an Internet Protocol (IP) or Bluetooth address, and capable of connecting directly or indirectly to the Internet.

The SB-327 bill, and related bills, are designed to protect devices and their information from "unauthorized access, destruction, use, modification, or disclosure." Note that there may be other similar bills in the near future originating in other states, or nationally. If so, Raritan will keep you informed in updated Technical Notes.

Raritan's Action Plan

To comply with SB-327, for Raritan's PDU products and for the PDU's firmware, the following plan has been implemented by Raritan, starting with Xerus firmware version 3.6.0 for January 2020.

- **What's new in Xerus firmware version 3.6.0:**

- Factory-default changes:
  - Only secure access (physical or by secure network protocols) is enabled by default.
  - During the first log in, before any service can be used, you are forced to change the default password.
- Configuration changes to enable insecure features provide a warning, require confirmation, and are logged.
- Configuring a PDU with factory settings via a USB drive requires using the set_password option, which changes the user's password before any commands can be executed. Access to units with factory settings will be denied unless the set_password option is used.

Default PDU configuration:

The factory default configuration has these services changed to disabled:

- SNMP Agent
- SCP interface (disabled until default password is changed)

The factory default configuration has these services remain enabled:

- HTTPS Server
- SSH Server
- Console

Notes:

Firmware updates to units in the field do not change any defaults until a reset to factory defaults occurs.

The network TCP/IP stack and DHCP remain enabled by default.

Default password change requirement:

The default password must be changed upon first use, before any other configuration changes or device access are allowed. In factory default configuration, the following protocols and tools, with the following restrictions, allow you to first update the default password:

- **HTTPS Server Web User Interface:**

- Restricted to a password change page/form only.

- **HTTPS Server (JSON API Web Service):**

- API limited to only system identification and a password change for the default account.

- **SSH Server:**

- Prompts for a password change.

- **Console:**

- Prompts for a password change.

Notes:

Once the default password is changed, the restrictions are removed and the PDU resumes normal operations for the protocols and tools listed above.

Upon any restart to factory defaults, the restrictions will again be enforced and a change to the default password will again be required.

PDU Automated Configuration, Bulk Configuration, and Provisioning

PDU automated configuration, bulk configuration, and provision processes are still supported by Xerus firmware version 3.6.0 PDUs in factory default configuration, although with restrictions and changes:

- If you are using your own automation and configuration tools to provision PDUs, you will have to accommodate the required changing of the password the first time you access the PDU.
- If you are using USB thumb drives for provisioning, a new password has to be provided by adding the "set_password" option to the configuration file.