Northwest Shelbyville
Regional Hospital

Memo

To:	CISO Chris Bailey
From:	John Kucera
Date:	10/29/2020
Re:	Vulnerabilities Discovered in Hospital Devices

Security vulnerabilities have been identified in two devices belonging to Northwest Shelbyville Regional Hospital. The first is Tinxy Door Lock with wifi Controller and Door Sensor, which is vulnerable to Replay Attacks that potentially allow an attacker to become an Authenticated User and gain control over the door lock. The second is Rubetek RV-3406/RV-3409/RV-3411 cameras, which are vulnerable to an attacker gaining access to camera live streams and camera settings without authentication.

Device 1: Tinxy Door Lock with wifi Controller and Door Sensor

Tinxy Door Lock is a smart door lock that can be locked remotely and reports opening and closing activity back to the owner. With Tinxy App, the respective mobile app, an Authenticated User can control the door lock remotely. The Authenticated User can also view door lock activity on Tinxy App for when the door has been locked or unlocked.

The device communicates with Tinxy App over wifi (MQTT Protocol). There is an offline mode in which the device communicates with the mobile app via WLAN (HTTP based requests). Tinxy App uses Authentication enforcement with phone number and email to whitelist Authenticated users. Non-authenticated users are implicitly denied device control but can send a request to the Homeowner to become an Authenticated User which the Homeowner must accept.

The known vulnerability was identified June 23, 2020 and published as CVE-2020-9438 in the National Vulnerability Database. An Authenticated User who has shared control with the Homeowner will have Offline Unlock and Lock requests sent in unprotected HTTP. An attacker, being a non-Authenticated User, can gain device control by intercepting the HTTP Unlock/Lock request and performing a Replay Attack in which the attacker uses the same request to Unlock/Lock the device. It has also been identified that the Replay Attack from the attacker continues to be successful even after the Homeowner removes Authentication from the original Authenticated User.

A solution that has been identified to fix the vulnerability is included in patched versions of Tinxy Door Lock Firmware Version 3.2 and Tinxy App Android Version 3.2.2. The patch details were unspecified, but the device still uses HTTP. Alternatively, the vulnerability can be fixed by switching from HTTP to HTTPS for communication between the device and Tinxy app. HTTP is vulnerable to Replay Attacks because there are no session keys to distinguish between transactions, and therefore the same Unlock/lock request can be repeated for the same result. However, HTTPS uses random session keys for encryption in Offline mode that HTTP does not normally provide. A Replay Attack will continue happening if the same session key is allowed for outsider access. To prevent this, both the device and Tinxy App should use random session keys that are valid only for one transaction each and reset to another randomized key for the next transaction. A Replay Attack will be unsuccessful if the intercepted key has expired.

I recommend that Northwest Shelbyville Regional Hospital avoid using Tinxy Door Lock with wifi Controller and Door Sensor. The patched version continues to use HTTP for offline communication between the device and Tinxy App which will always lack protection over data in comparison to HTTPS. This organization should replace Tinxy Door Lock with a smart door lock that uses HTTPS instead of HTTP for offline mode. An alternative replacement is using a smart door lock does not allow offline remote control such as Ultraloq U-Bolt Pro. Ultraloq U-Bolt Pro has versatile offline door unlocking in which the user can user a fingerprint scan, keypad, or physical key to unlock the door. With no offline remote control allowed, attackers cannot intercept unprotected HTTP requests. The security risk of offline remote control outweighs its convenience.

Additionally, a policy should be enforced that forbids smart devices using HTTP. The vulnerability should be avoided across all device implementations at Northwest Shelbyville Regional Hospital.

Device 2: Rubetek RV-3406, RV-3409, and RV-3411 cameras (firmware versions v342, v339)

Rubetek RV-3406, RV-3409, and RV-3411 cameras are smart security cameras that can be remotely controlled and monitored. Rubetek cameras live stream the surveillance to the user on their computer with RTSP (Real Time Streaming Protocol). The user can also remotely change settings including camera rotation, brightness, clarity, date/time, camera restart, and resetting to factory settings. Additionally, Rubetek cameras support ONVIF services which allow surveillance devices from different manufacturers to be standardized and operate together. Authentication and data communication between Rubetek cameras and the user’s system are provided through Telnet Protocol which transfers data in plain text.

The known vulnerability was identified September 25, 2020 and published as CVE-2020-25747 in the National Vulnerability Database. The Rubetek Cameras use Telnet which is unencrypted and requires no authentication. Any remote attacker can intercept transmissions in order to control the devices with little effort. There is authentication required to access the devices, but it can be easily found by looking at the plain text communications between the devices and the user’s system. Attackers will gain control over the RTSP allowing them to view the camera live stream. They will also be able to view and alter settings including camera rotation, brightness, clarity, date/time, camera restart, and resetting to factory settings. Additionally, attackers will have access to the ONVIF services which potentially gives them control over non-Rubetek ONVIF-supporting cameras controlled by the same system.

There are no known fixed versions yet for these Rubetek Cameras. A possible solution to fix the vulnerability is to use SSH Protocol instead of Telnet. SSH provides the same remote data communication service as Telnet but with stronger security. SSH uses public key encryption, so only authenticated users will be allowed to remotely access the camera’s data communications. SSH also sends all data in an encrypted format, as opposed to Telnet’s plain text, so external entities would not be able to read the camera’s data communication if they intercept.

I recommend that Northwest Shelbyville Regional Hospital avoid using Rubetek RV-3406, RV-3409, and RV-3411 cameras. Telnet transmits data with too little security and attackers could gain control over the cameras with little effort. The organization should replace these cameras with a different brand of smart security cameras that do not use Telnet. Additionally, a policy should be enforced that forbids smart devices using Telnet. The vulnerability should be avoided across all device implementations at Northwest Shelbyville Regional Hospital.

The safest solution, although less convenient, would be to avoid the use of smart security cameras altogether. Dumb surveillance cameras are more secure than smart ones as their data cannot be intercepted remotely. Although dumb security cameras do not provide live streaming, they still provide their main service of storing surveillance footage for future viewing. Smart security cameras make it easy to monitor the building, but the security risk outweighs the convenience. Door sensors and human security guards are more effective for actively monitoring the Hospital indoors.

References

Jet-Pentest. (2020, September 18). Jet-pentest/CVE-2020-25747. Retrieved October 29, 2020, from https://github.com/jet-pentest/CVE-2020-25747

National Institute of Standards and Technology. (2020, June 23). National Vulnerability Database. Retrieved October 29, 2020, from https://nvd.nist.gov/vuln/detail/CVE-2020-9438

National Institute of Standards and Technology. (2020, September 25). National Vulnerability Database. Retrieved October 29, 2020, from https://nvd.nist.gov/vuln/detail/CVE-2020-25747

Raychoudhury, A. (2020, June 25). Smart Products are always not that smart...... Tinxy Smart Door Lock Vulnerability.. Retrieved October 29, 2020, from https://medium.com/@avishek_75733/smart-products-are-always-not-that-smart-tinxy-smart-door-lock-vulnerability-97f91e435e06

Ultraloq. (2019, August 13). Ultraloq U-Bolt Pro Bluetooth Enabled Fingerprint and Keypad Smart Deadbolt. Retrieved October 29, 2020, from https://store.u-tec.com/products/ultraloq-u-bolt-pro-bluetooth-enabled-fingerprint-and-keypad-smart-deadbolt