PRODUCT SECURITY ADVISORY

June 02, 2022

PSIRT Record Number
CARR-PSA-006-0622

Overview

By use of our responsible disclosure procedures independent penetration testing of HID® Mercury™, access panels sold by LenelS2 were reported to contain cybersecurity vulnerabilities. These vulnerabilities could lead to disruption of normal panel operations.

The impacted LenelS2 part numbers include:

LNL-X2210
LNL-X2220
LNL-X3300
LNL-X4420
LNL-4420
S2-LP-1501
S2-LP-1502
S2-LP-2500
S2-LP-4502

Prior generations of HID Mercury controllers are not impacted.

PSIRT Statement

The following table provides the nature of the vulnerability found and which firmware release addresses the issue:

CVE	CWE	"X", "S2" Series	LNL-4420
CVE-2022-31479	CWE-693 Protection Mechanism Failure	1.302	1.296
CVE-2022-31480	CWE-425 Direct Request (Forced Browsing)	1.302	1.296
CVE-2022-31481	CWE-120 Buffer Overflow	1.302	1.296
CVE-2022-31482	CWE-120 Buffer Overflow	1.29	1.29
CVE-2022-31483	CWE-22 Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	1.271	1.271
CVE-2022-31484	CWE-425 Direct Request (Forced Browsing)	1.29	1.29
CVE-2022-31485	CWE-425 Direct Request (Forced Browsing)	1.29	1.29
CVE-2022-31486	CWE-78 OS Command Injection	1.303	1.297

Remediation

Updating these access panels to the most current released firmware via the LenelS2 Partner Center. Please contact your support channel partner for instructions.

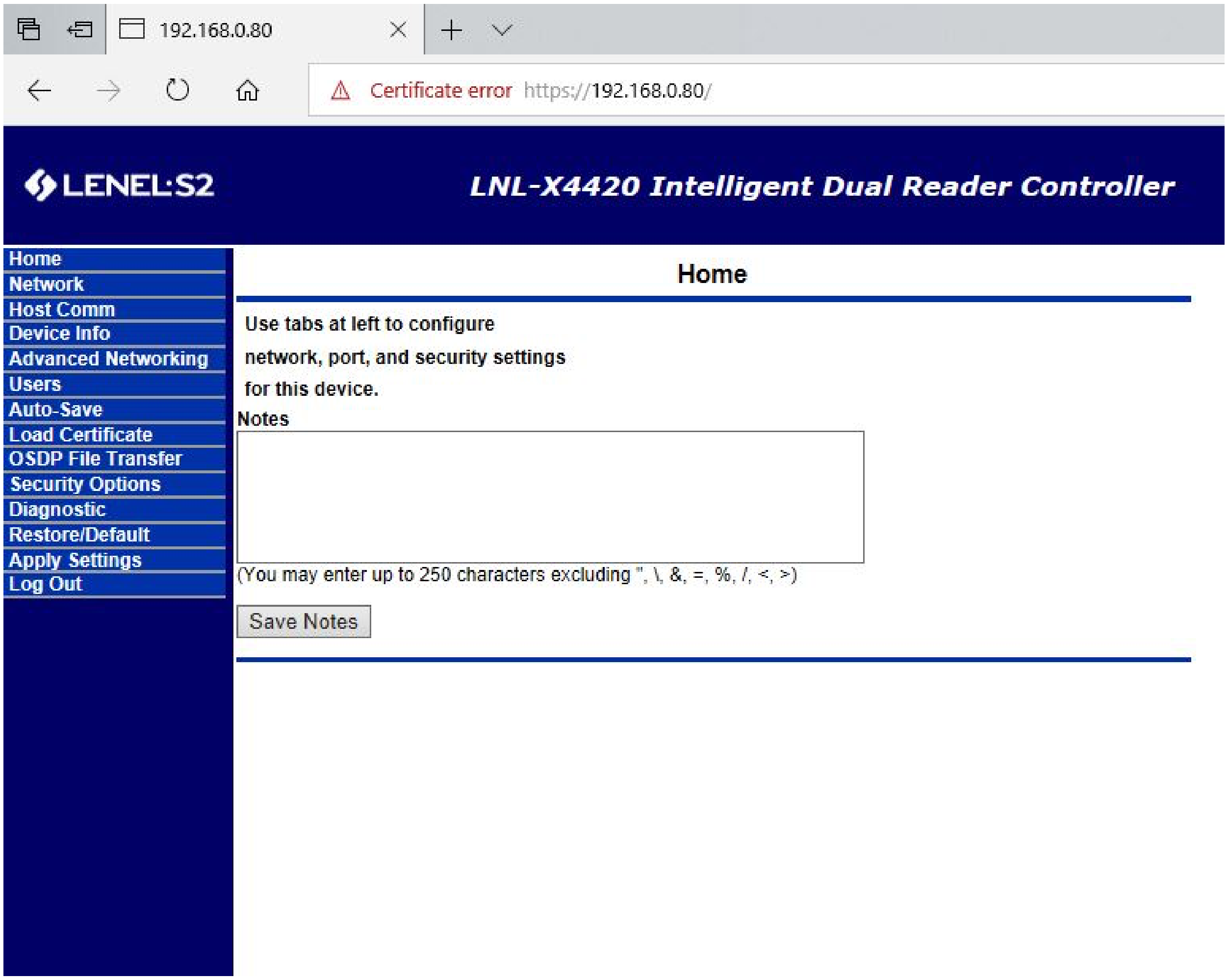
Mitigation

NOTE: When the controller is configured to disable web access, you cannot remotely login into the controller's web page. To log in, physically turn Switch 1 to “on” at the controller, and login within 5 minutes.

Procedure to disable Controller Web Login

1. Login to controller web pages

2. Go to “Users” Tab

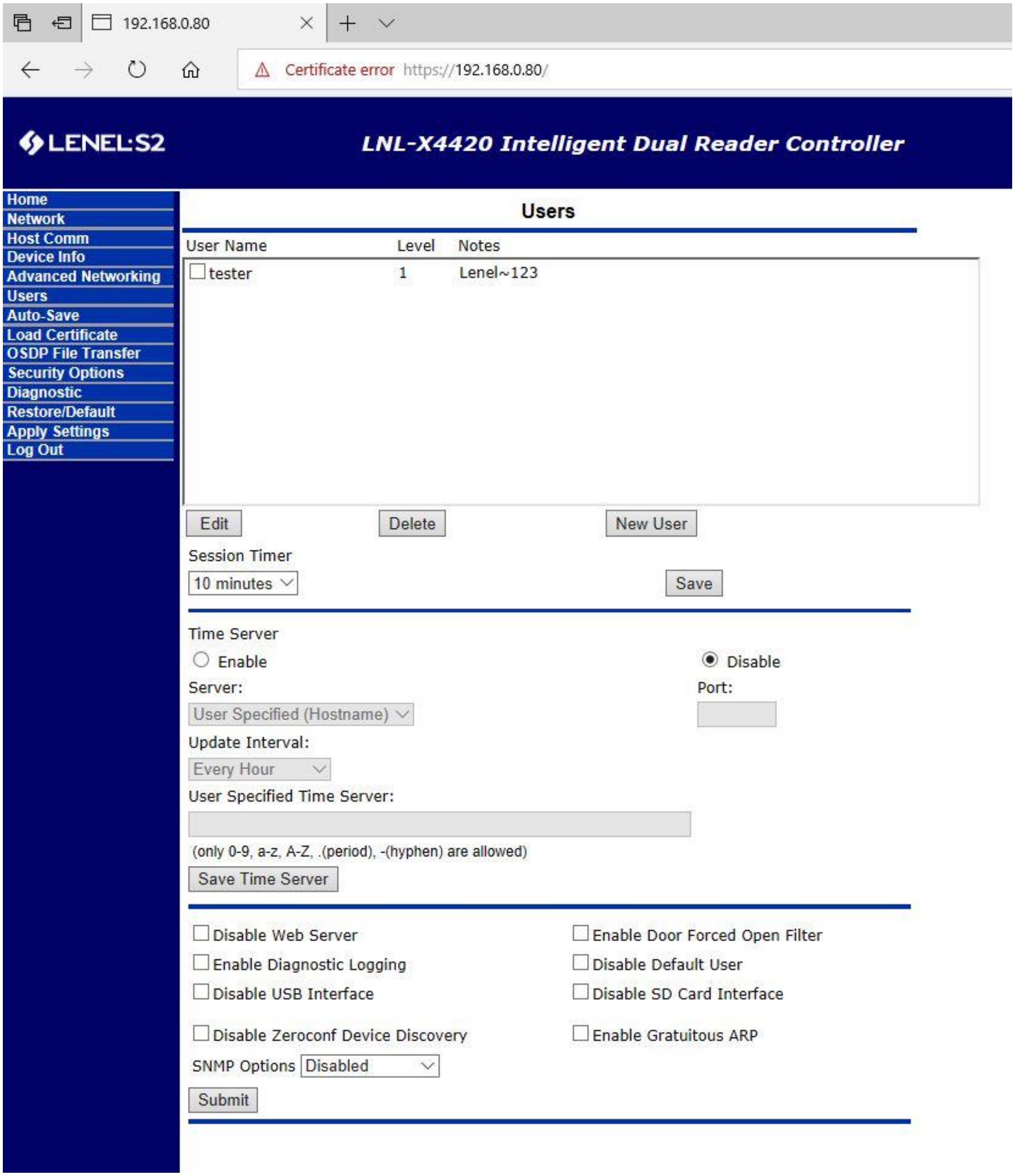


Use tabs at left to configure network, port, and security settings for this device.

(You may enter up to 250 characters excluding ", \, &, =, %, /, <, >)

3. Near bottom of the users page, check option to “Disable Web Server”

4. Select “Submit” at the bottom of the page



LNL-X4420 Intelligent Dual Reader Controller

Users

User Name	Level	Notes
□ tester	1	Lenel~123

Session Timer: 10 minutes

Time Server

○ Enable ● Disable

Server: User Specified (Hostname)

Port:

Update Interval: Every Hour

User Specified Time Server:

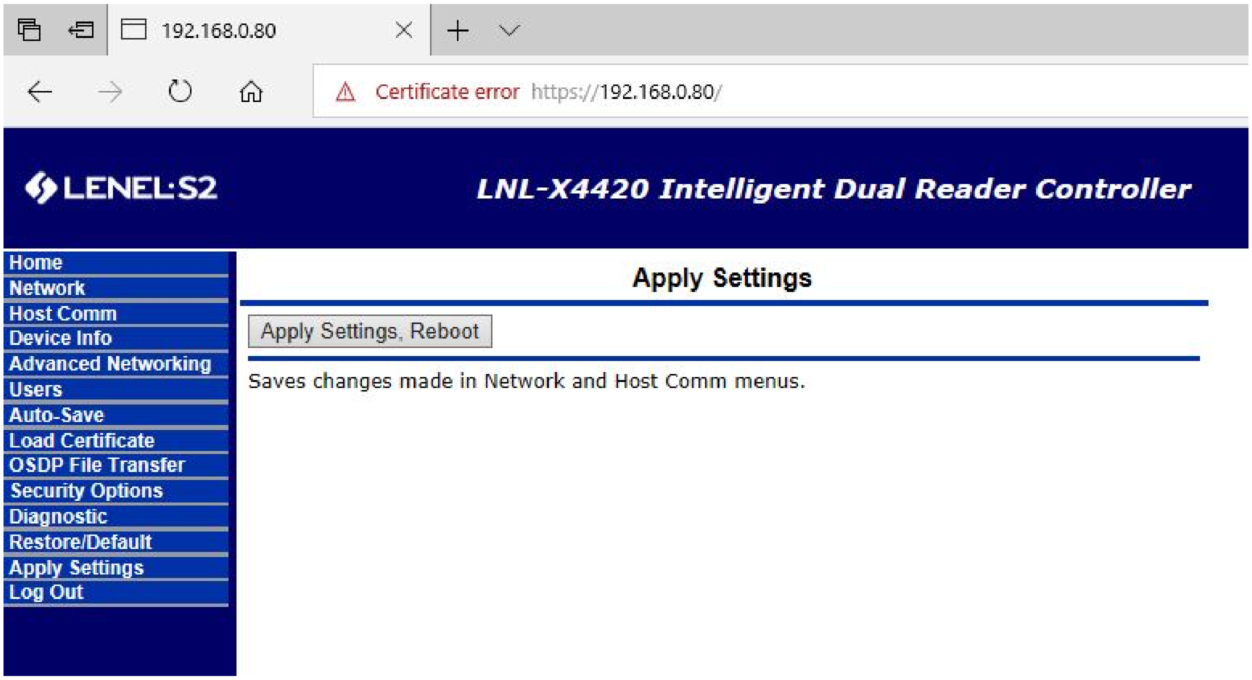
(only 0-9, a-z, A-Z, .(period), -(hyphen) are allowed)

□ Disable Web Server
□ Enable Diagnostic Logging
□ Disable USB Interface
□ Disable Zeroconf Device Discovery
□ Enable Door Forced Open Filter
□ Disable Default User
□ Disable SD Card Interface
□ Enable Gratuitous ARP

SNMP Options: Disabled

5. Select “Apply Settings” tab

6. On that page, select “Apply Settings, Reboot”



Saves changes made in Network and Host Comm menus.

The controller will apply the new setting and reboot. Web login will be disabled until Switch 1 is physically turned “On,” on the controller.

About Carrier Global Product Cybersecurity

At Carrier, system and operational security is integral. To ensure outcomes, research and development teams leverage Global Product Cybersecurity – a team of highly experienced and credentialed veterans; diverse and dynamic cybersecurity domain experts who’ve maintained prominent roles and responsibilities in designing, building, and operating highly secure complex systems.

The Product Security Incident Response Team (PSIRT) focuses on the identification, assessment, and disposition of the risks associated with security vulnerabilities within Carrier products, offerings, solutions, components and/or services. PSIRT is a dedicated team of first responders responsible to deliver advanced support designed to contain and minimize the spread and impact of a product security event, incident, breach, and/or crises.

For more information about Global Product Security and PSIRT, please visit us at: https://www.corporate.carrier.com/product-security/

Or you may contact us at: productsecurity@carrier.com

Initial Publication Date	Last Published Date
June 02, 2022	June 02, 2022