Honeywell

SECURITY NOTICE

SN 2022-06-02 #01: MULTIPLE VULNERABILITIES IN HID® Mercury™ Intelligent Controllers - (CVE-2022-31479, CVE-2022-31480, CVE-2022-31481, CVE-2022-31482, CVE-2022-31483, CVE-2022-31484, CVE-2022-31485, CVE-2022-31486)

This article contains:

It applies to:

All LenelS2 products integrated with HID® Mercury™ Intelligent Controllers: LNL-X2210, LNL-X2220, LNL-X3300, LNL-X4420, LNL-4420, S2-LP-1501, S2-LP-1502, S2-LP-2500, S2-LP-4502

Executive Summary

Honeywell is aware of multiple vulnerabilities reported by an independent penetration test of HID® Mercury™ Intelligent Controllers sold by LenelS2. These vulnerabilities could lead to a disruption of normal panel operations.

Honeywell strongly recommends that users upgrade to the latest available firmware for their respective Intelligent Controllers mentioned below to resolve the vulnerability.

Honeywell

Vulnerability Synopsis

1. OS Command Injection in HID® Mercury™ Intelligent Controllers – (CVE-2022-31479)

   An unauthenticated attacker can update the hostname with a specially crafted name that will allow for shell commands to be executed during the core collection process. This vulnerability impacts products based on HID Mercury Intelligent Controllers LP1501, LP1502, LP2500, LP4502, and EP4502 which contain firmware versions prior to 1.302 for the LP series and 1.296 for the EP series. An attacker with this level of access on the device can monitor all communications sent to and from this device, modify onboard relays, change configuration files, or cause the device to become unstable. The injected commands only get executed during start up or when unsafe calls regarding the hostname are used. This allows the attacker to gain remote access to the device and can make their persistence permanent by modifying the filesystem.

   CVSS Base Score: 9.6 Critical

   CVSS Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:H/I:H/A:H

   CVE Number: CVE-2022-31479

   https://nvd.nist.gov/vuln/detail/CVE-2022-31479

2. Unauthenticated Firmware Upload in HID® Mercury™ Intelligent Controllers – (CVE-2022-31480)

   An unauthenticated attacker could arbitrarily upload firmware files to the target device, ultimately causing a Denial-of-Service (DoS). This vulnerability impacts products based on HID Mercury Intelligent Controllers LP1501, LP1502, LP2500, LP4502, and EP4502 which contain firmware versions prior to 1.302 for the LP series and 1.296 for the EP series. The attacker needs to have a properly signed and encrypted binary, loading the firmware to the device ultimately triggers a reboot.

   CVSS Base Score: 7.5 High

   CVSS Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H

   CVE Number: CVE-2022-31480

   https://nvd.nist.gov/vuln/detail/CVE-2022-31480

3. Buffer Overflow in HID® Mercury™ Intelligent Controllers - (CVE-2022-31481)

   An unauthenticated attacker can send a specially crafted update file to the device that can overflow a buffer. This vulnerability impacts products based on HID Mercury Intelligent Controllers LP1501, LP1502, LP2500, LP4502, and EP4502 which contain

firmware versions prior to 1.302 for the LP series and 1.296 for the EP series. The overflowed data can allow the attacker to manipulate the “normal” code execution to that of their choosing. An attacker with this level of access on the device can monitor all communications sent to and from this device, modify onboard relays, change configuration files, or cause the device to become unstable.

CVSS Base Score: 10.0 Critical

CVSS Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H

CVE Number: CVE-2022-31481

https://nvd.nist.gov/vuln/detail/CVE-2022-31481

4. Buffer Overflow in HID® Mercury™ Intelligent Controllers - (CVE-2022-31482)

An unauthenticated attacker can send a specially crafted unauthenticated HTTP request to the device that can overflow a buffer. This vulnerability impacts products based on HID Mercury Intelligent Controllers LP1501, LP1502, LP2500, LP4502, and EP4502 which contain firmware versions prior to 1.29. The overflowed data leads to segmentation fault and ultimately a denial-of-service condition, causing the device to reboot. The impact of this vulneraccability is that an unauthenticated attacker could leverage this flaw to cause the target device to become unresponsive. An attacker could automate this attack to achieve persistent DoS, effectively rendering the target controller useless.

CVSS Base Score: 9.0 Critical

CVSS Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H

CVE Number: CVE-2022-31482

https://nvd.nist.gov/vuln/detail/CVE-2022-31482

5. Path Traversal in HID® Mercury™ Intelligent Controllers - (CVE-2022-31483)

An authenticated attacker can upload a file with a filename including “..” and “/” to achieve the ability to upload the desired file anywhere on the filesystem. This vulnerability impacts products based on HID Mercury Intelligent Controllers LP1501, LP1502, LP2500, LP4502, and EP4502 which contain firmware versions prior to 1.271. This allows a malicious actor to overwrite sensitive system files and install a startup service to gain remote access to the underlaying Linux operating system with root privileges.

CVSS Base Score: 9.1 Critical

CVSS Vector: CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:C/C:H/I:H/A:H

CVE Number: CVE-2022-31483

https://nvd.nist.gov/vuln/detail/CVE-2022-31483

6. Unauthenticated User Manipulation in HID® Mercury™ Intelligent Controllers - (CVE-2022-31484)

   An unauthenticated attacker can send a specially crafted network packet to delete a user from the web interface. This vulnerability impacts products based on HID Mercury Intelligent Controllers LP1501, LP1502, LP2500, LP4502, and EP4502 which contain firmware versions prior to 1.29. The impact of this vulnerability is that an unauthenticated attacker could restrict access to the web interface to legitimate users and potentially requiring them to use the default user dip switch procedure to gain access back.

   CVSS Base Score: 7.5 High

   CVSS Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H

   CVE Number: CVE-2022-31484

   https://nvd.nist.gov/vuln/detail/CVE-2022-31484

7. Unauthenticated Changes to Web Interface in HID® Mercury™ Intelligent Controllers - (CVE-2022-31485)

   An unauthenticated attacker can send a specially crafted packets to update the “notes” section of the home page of the web interface. This vulnerability impacts products based on HID Mercury Intelligent Controllers LP1501, LP1502, LP2500, LP4502, and EP4502 which contain firmware versions prior to 1.29.

   CVSS Base Score: 5.3 Medium

   CVSS Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:N

   CVE Number: CVE-2022-31485

   https://nvd.nist.gov/vuln/detail/CVE-2022-31485

8. OS Command Injection in HID® Mercury™ Intelligent Controllers - (CVE-2022-31486)

   An authenticated attacker can send a specially crafted route to the “edit_route.cgi” binary and have it execute shell commands. This vulnerability impacts products based on HID Mercury Intelligent Controllers LP1501, LP1502, LP2500, LP4502, and EP4502 which contain firmware versions prior to 1.303 for the LP series and 1.297 for the EP series. An attacker with this level of access on the device can monitor all communications sent to and from this device, modify onboard relays, change configuration files, or cause the device to become unstable.

   CVSS Base Score: 8.8 High

CVSS Vector: CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

CVE Number: CVE-2022-31486

https://nvd.nist.gov/vuln/detail/CVE-2022-31486

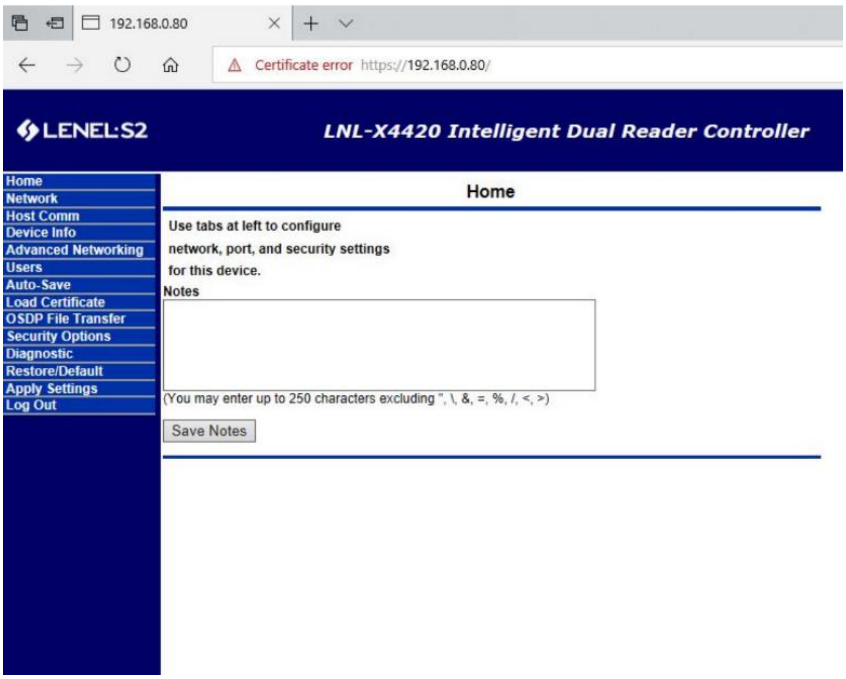
Mitigation

Mitigation is strongly recommended until the appropriate firmware upgrade can be installed or if users cannot install it.

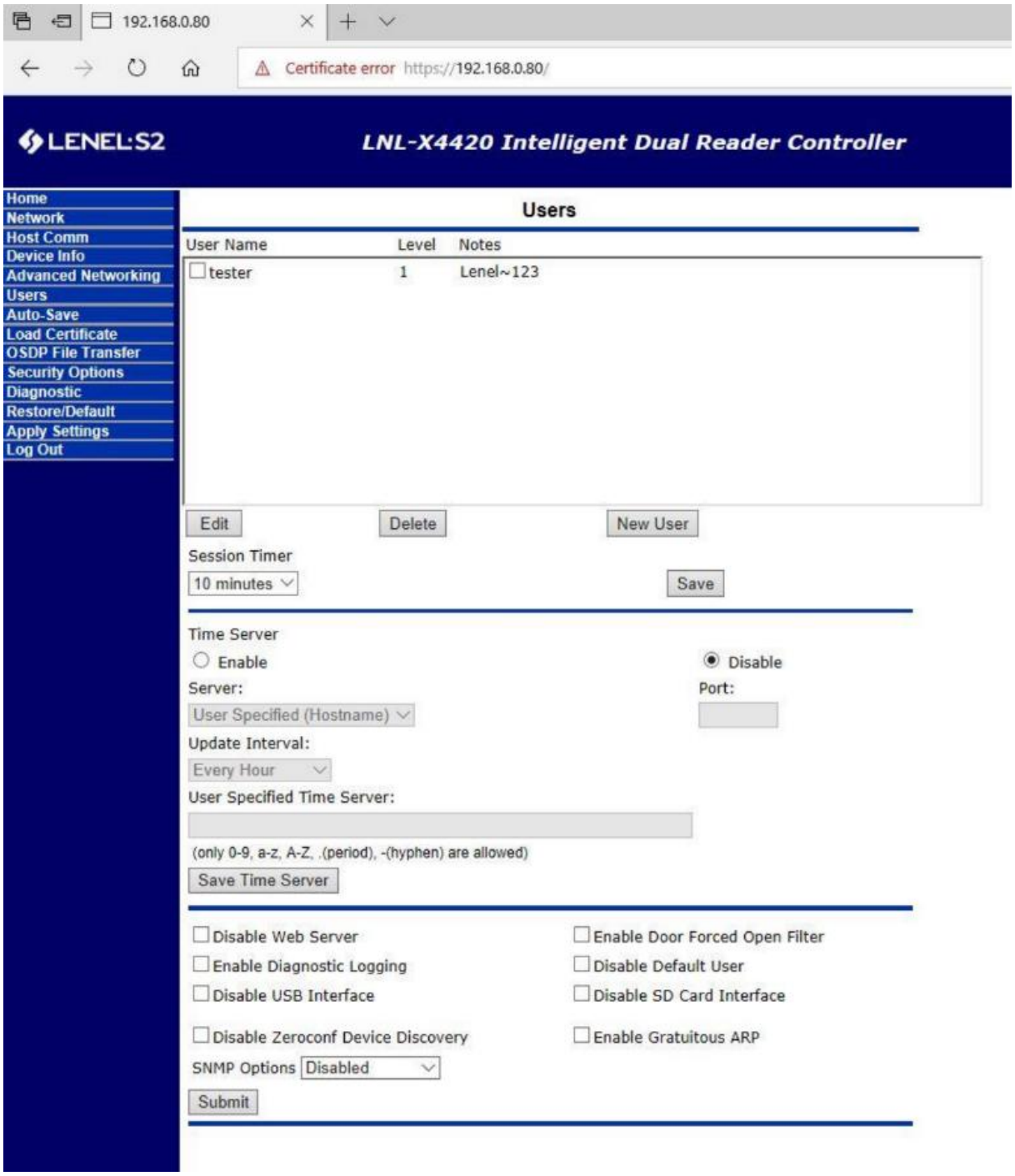
NOTE: When the controller is configured to disable web access, you cannot remotely log into the controller's web page. To log in, physically turn Switch 1 to "on" at the controller, and login within 5 minutes.

Procedure to disable Controller Web Login

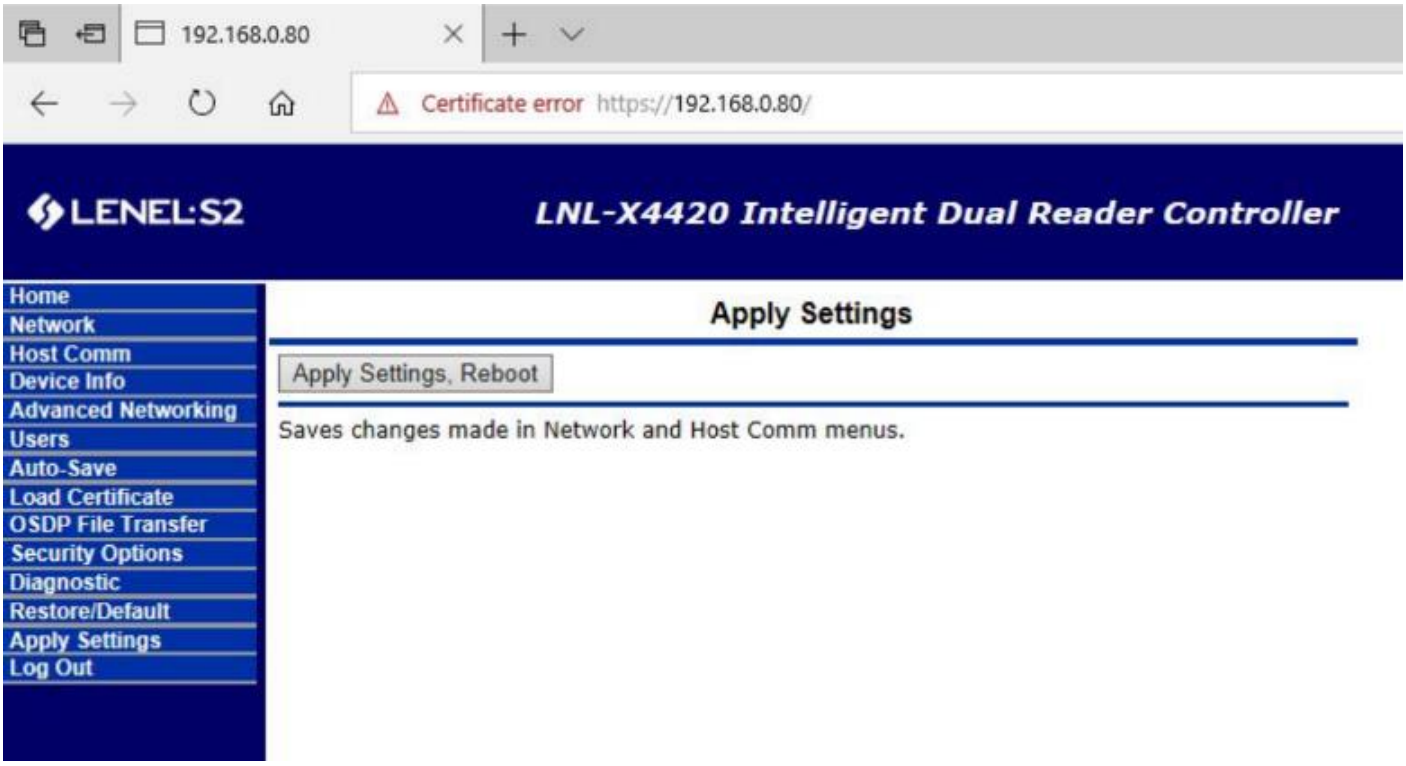
1. Login to controller web pages
2. Go to "Users" Tab



3. Near bottom of the user's page, check option to "Disable Web Server"
4. Select "Submit" at the bottom of the page



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



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

CAUTION: Due to the wide variety of process control equipment configurations and site-specific control strategies, it is the responsibility of each customer to assess the potential impact of this anomaly to their process & facilities.

Affected Products

Product	Advisory/Update
LNL-X2210, LNL-X2220, LNL-X3300, LNL-X4420	**Update these Intelligent Controllers to the most current released firmware via the LenelS2 Partner Center.** *Please contact your support channel partner for instructions.*
LNL-4420	
S2-LP-1501, S2-LP-1502, S2-LP-2500, S2-LP-4502	

Prior generations of HID® Mercury™ Intelligent Controllers were not impacted.

Remediation

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

CVE	"X" & "S2" Series	LNL-4420
CVE-2022-31479	1.302	1.296
CVE-2022-31480	1.302	1.296
CVE-2022-31481	1.302	1.296
CVE-2022-31482	1.29	1.29
CVE-2022-31483	1.271	1.271
CVE-2022-31484	1.29	1.29
CVE-2022-31485	1.29	1.29
CVE-2022-31486	1.303	1.297

Honeywell strongly recommends that users update these Intelligent Controllers to the most current released firmware via the LenelS2 Partner Center.

Please contact your support channel partner for instructions.

References

- https://nvd.nist.gov/vuln/detail/CVE-2022-31479
- https://nvd.nist.gov/vuln/detail/CVE-2022-31480
- https://nvd.nist.gov/vuln/detail/CVE-2022-31481
- https://nvd.nist.gov/vuln/detail/CVE-2022-31482
- https://nvd.nist.gov/vuln/detail/CVE-2022-31483
- https://nvd.nist.gov/vuln/detail/CVE-2022-31484
- https://nvd.nist.gov/vuln/detail/CVE-2022-31485
- https://nvd.nist.gov/vuln/detail/CVE-2022-31486

Honeywell

Appendix: About CVSS

The Common Vulnerability Scoring System (CVSS) is an open standard for communicating the characteristics and severity of software vulnerabilities. The Base score represents the intrinsic qualities of a vulnerability. The Temporal score reflects the characteristics of a vulnerability that change over time. The Environmental score is an additional score that can be used by CVSS, but is not supplied as it will differ for each customer.

The Base score has a value ranging from 0 to 10. The Temporal score has the same range and is a modification of the Base score due to current temporary factors.

The severity of the score can be summarized as follows:

Severity Rating	CVSS Score
None	0.0
Low	0.1 – 3.9
Medium	4.0 – 6.9
High	7.0 – 8.9
Critical	9.0 – 10.0

A CVSS score is also represented as a vector string, a compressed textual representation of the values used to derive the score.

Detailed information about CVSS can be found at http://www.first.org/cvss.

DISCLAIMERS

- CUSTOMERS ARE RESPONSIBLE FOR ASSESSING THE IMPACT OF ANY ACTUAL OR POTENTIAL SECURITY VULNERABILITY. CUSTOMER'S FAILURE TO IMPLEMENT THE RECOMMENDED UPDATES OR ACTIONS, INCLUDING WITHOUT LIMITATION, RECOMMENDED PATCHES OR UPDATES TO ANY SOFTWARE OR DEVICE, SHALL BE AT CUSTOMER'S SOLE RISK AND EXPENSE. CUSTOMER SHALL TAKE ALL APPROPRIATE ACTIONS TO SECURE AND SAFEGUARD ITS SYSTEMS AND DATA. HONEYWELL SHALL HAVE NO LIABILITY FOR (I) CUSTOMER'S FAILURE TO IMPLEMENT THE RECOMMENDED UPDATES OR ACTIONS OR (II) CUSTOMER'S FAILURE TO SECURE AND **SAFEGUARD ITS SYSTEMS AND DATA. SUCH FAILURES CAN VOID HONEYWELL'S WARRANTY OBLIGATIONS.**
- YOUR USE OF THE INFORMATION ON THIS DOCUMENT OR MATERIALS LINKED FROM THIS DOCUMENT IS AT YOUR OWN RISK.
- HONEYWELL RESERVES THE RIGHT TO CHANGE OR UPDATE THIS DOCUMENT AT ANY TIME AND WITHOUT NOTICE.
- HONEYWELL PROVIDES THE CVSS SCORES "AS IS" WITHOUT WARRANTY OF ANY KIND. HONEYWELL DISCLAIMS THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PURPOSE AND MAKES NO EXPRESS WARRANTIES EXCEPT AS MAY BE STATED IN A WRITTEN AGREEMENT WITH AND FOR ITS CUSTOMERS
- IN NO EVENT WILL HONEYWELL BE LIABLE TO ANYONE FOR ANY DIRECT, INDIRECT, SPECIAL, OR CONSEQUENTIAL DAMAGES.