Honeywell

SECURITY NOTICE

SN 2024-05-24 #01: VULNERABILITIES IN LENELS2 NETBOX - (CVE-2024-2420, CVE-2024-2421, CVE-2024-2422)

This article contains:

It applies to:

NetBox

Executive Summary

Honeywell is aware of multiple vulnerabilities affecting the LenelS2 NetBox.

The vulnerability assigned CVE-2024-2420 is rated with a severity of High and has been published as a CWE-259: Use of Hard-coded Password. This vulnerability allows an attacker to bypass authentication requirements.

The vulnerability assigned CVE-2024-2421 is rated with a severity of Critical and has been published as a CWE-78: Improper Neutralization of Special Elements used in an OS Command (‘OS Command Injection’). This vulnerability allows an attacker to execute malicious commands with elevated permissions.

The vulnerability assigned CVE-2024-2422 is rated with a severity of Critical and has been published as a CWE-88: Improper Neutralization of Argument Delimiters in a Command (‘Argument Injection’). This vulnerability allows an attacker to execute malicious commands.

Honeywell strongly recommends that users upgrade to the version identified below to resolve the vulnerabilities.

Vulnerability Synopsis

1. Hardcoded Credentials in LenelS2 NetBox – (CVE-2024-2420)

   LenelS2 NetBox access control and event monitoring system was discovered to contain Hardcoded Credentials in versions prior to and including 5.6.1 which allows an attacker to bypass authentication requirements.

   CVSS Base Score: 8.8 High

   CVSS Vector: CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:H/VI:L/VA:L/SC:N/SI:N/SA:N

   CVE Number: CVE-2024-2420

   https://nvd.nist.gov/vuln/detail/CVE-2024-2420

2. Un-authenticated RCE in LenelS2 NetBox - (CVE-2024-2421)

   LenelS2 NetBox access control and event monitoring system was discovered to contain an unauthenticated RCE in versions prior to and including 5.6.1, which allows an attacker to execute malicious commands with elevated permissions.

   CVSS Base Score: 9.3 Critical

   CVSS Vector: CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N

   CVE Number: CVE-2024-2421

   https://nvd.nist.gov/vuln/detail/CVE-2024-2421

3. Authenticated RCE in LenelS2 NetBox - (CVE-2024-2422)

   LenelS2 NetBox access control and event monitoring system was discovered to contain an authenticated RCE in versions prior to and including 5.6.1, which allows an attacker to execute malicious commands.

   CVSS Base Score: 9.3 Critical

   CVSS Vector: CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N

   CVE Number: CVE-2024-2420

   https://nvd.nist.gov/vuln/detail/CVE-2024-2422

Affected Products

Product	CVE	Advisory/Update
NetBox versions prior to v5.6.2	CVE-2024-2420 CVE-2024-2421 CVE-2024-2422	**Upgrade to NetBox v5.6.2**

Remediation

These vulnerabilities have been remediated in NetBox™ release 5.6.2.

Honeywell strongly recommends that users upgrade to NetBox™ release 5.6.2 by contacting their authorized installer.

Users should follow recommended deployment guidelines found in the NetBox hardening guide found in the NetBox built-in help menu.

References

- https://nvd.nist.gov/vuln/detail/CVE-2024-2420
- https://nvd.nist.gov/vuln/detail/CVE-2024-2421
- https://nvd.nist.gov/vuln/detail/CVE-2024-2422

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.