PRODUCT SECURITY ADVISORY

CARR-PSA-2024-01

May 30, 2024

LenelS2 NetBox™

Overview

Carrier is aware of vulnerabilities impacting Lenel2 NetBox™.

NetBox™ is a full-featured, browser-based access control and event monitoring system.

Successful exploitation of these vulnerabilities could allow an attacker to bypass authentication and execute malicious commands with elevated permissions.

Affected Products

Product	Version
LenelS2 NetBox™	**All versions prior to 5.6.2**

Vulnerability Details

CVE ID	CVSS v3.1	Severity	CVSS v4.0	Severity
CVE-2024-2420	Base Score 9.8	Critical	Base Score 8.8	High
CVE-2024-2421	Base Score 9.1	Critical	Base Score 9.3	Critical
CVE-2024-2422	Base Score 8.6	High	Base Score 9.3	Critical

CVE ID: **CVE-2024-2420**

CVSS v3.1 Base Score 9.8 Critical CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

CVSS v4.0 Base Score 8.8 High AV:N/AC:L/AT:N/PR:N/UI:N/VC:H/VI:L/VA:L/SC:N/SI:N/SA:N

CWE-259 *Use of Hard-Coded Password* vulnerability exists which could allow an attacker to bypass authentication requirements.

CVE ID: **CVE-2024-2421**

CVSS v3.1 Base Score 9.1 Critical CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:C/C:H/I:H/A:H

CVSS v4.0 Base Score 9.3 Critical AV:N/AC:L/AT:N/PR:N/UI:N/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N

CWE-78 *Improper Neutralization of Special Elements Used In An OS Command* unauthenticated remote code execution exists which could allow an attacker to execute malicious commands with elevated permissions.

CVE ID: **CVE-2024-2422**

CVSS v3.1 Base Score 8.8 High CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

CVSS v4.0 Base Score 9.3 Critical AV:N/AC:L/AT:N/PR:N/UI:N/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N

CWE-88 *Improper Neutralization of Argument Delimiters In A Command (‘Argument Injection’)* authenticated remote code execution exists which could allow an attacker to execute malicious commands.

Remediation

These vulnerabilities have been mitigated in NetBox™ release 5.6.2. It is strongly recommended that customers upgrade to NetBox™ release 5.6.2 by contacting their authorized installer.

Mitigation

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

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
05-30-2024	05-30-2024