SECURITY NOTICE

SN2026-08-05: Copy Fail Vulnerability in LenelS2 NetBox Appliances - CVE-2026-31431

This article contains:

It applies to:

NetBox and NetBox Global appliances

Executive Summary

Following an investigation of CVE-2026-31431, Honeywell determined that this vulnerability poses no direct risk to NetBox deployments where end users and system integrators lack local command-line or shell access.

CVE-2026-31431 is a local privilege escalation vulnerability that requires the ability to execute arbitrary local code and interact directly with specific kernel interfaces. These conditions are not met in the current environment, where access is restricted and protected by PIN authentication.

As a result, the known exploit path is effectively blocked and cannot be triggered through the web interface, remote network access, or normal user activity. Residual risk is limited to highly trusted technical service accounts, for which temporary hardening measures, such as disabling the algif_aead kernel module, are being applied until a patched kernel is delivered in NetBox v6.4.1 and NetBox Global v4.0.3.

Vulnerability Synopsis

CVE Number	CVE-2026-31431
CVSS Severity Score	7.8 - High
Ubuntu Priority	High
Ubuntu Security Reference	Ubuntu Security CVE-2026-31431

Affected Products

Product	Advisory/Update
NetBox Global 4.0.3	**Not Vulnerable**
NetBox Global 4.0.x	**Upgrade to Global 4.0.3**
NetBox Global 3.1.x	**Migrate to Global 4.0.3**
NetBox v6.4.1	**Not Vulnerable**
NetBox v6.4.0	**Upgrade to NetBox v6.4.1**
NetBox v6.2.x	**Upgrade to NetBox v6.4.1**
NetBox v6.0.x	**Upgrade to NetBox v6.4.1**
NetBox v5.6.3 UB18 and earlier	**Upgrade to NetBox v6.4.1**
NetBox v5.6.3 UB16 and earlier	**Forward Upgrade Hardware Program**

Remediation

Honeywell strongly recommends that users upgrade to NetBox v6.4.1 and NetBox Global 4.0.3 as soon as possible.

For deployments that cannot immediately upgrade, residual exposure is limited to highly trusted technical service accounts with local command-line or shell access. For NetBox converged appliances, VRx and NetVR, contact Technical Support for assistance.

Systems identified for the Forward Upgrade Hardware Program should follow that program path to move to supported hardware and software capable of receiving the recommended update.