PRODUCT SECURITY ADVISORY

March 16, 2023

PSIRT Record Number
CARR-PSA-011-0323

Overview

A vulnerability discovered in a third-party tool, Apache HTTP Server mod_proxy (CVE-2021-40438), is published as a CWE-918: Server-Side Request Forgery (SSRF), which affects Apache HTTP Server versions 2.4.48 and earlier.

PSIRT Statement

Apache HTTP Server version 2.4.29 was released with the following LenelS2 supported platform versions using Ubuntu 16 UPG3:

- NetBox, NetVR, (including converged NetBox/VR, NetBox/VRx, and Quatro) – versions 5.4.5 & 5.6.0
- NetBox Global – version 3.1.2
- VRx – version 5.5.1

LenelS2 has prepared updates for each affected version of its platforms remediating the vulnerability contained in Apache HTTP Server. These updates may be found in LenelS2 Support Central by the following version numbers:

- NetBox, NetVR, (including converged NetBox/VR, NetBox/VRx, and Quatro) – versions 5.4.6 & 5.6.0.316
- NetBox Global – version 3.1.3 (contact Technical Support for assistance)
- VRx – version 5.5.2

LenelS2 advises customers to apply these updated versions as soon as possible.

Customers using earlier unsupported versions of LenelS2 platforms not listed above should verify their Ubuntu version. If Ubuntu 16 UPG3 is used, customers should upgrade to the latest LenelS2 version.

Carrier is rapidly working to determine if any additional offerings may be impacted by the Apache HTTP Server mod_proxy SSRF vulnerability. Should we determine that any of our offerings were impacted, additional information regarding mitigations or other actions in response to this matter will follow as our investigation unfolds. More information about the vulnerability is provided by the Apache HTTP Servier Project:

https://httpd.apache.org/security/vulnerabilities_24.html#2.4.49

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 as: https://www.corporate.carrier.com/product-security/

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

Initial Publication Date	Last Published Date
March 13, 2023	March 16, 2023