PRODUCT SECURITY ADVISORY

December 16, 2022

PSIRT Record Number
CARR-PSA-007-1122

Overview

On October 13, 2022, CVE-2022-42889 was published as a Remote Code Execution vulnerability effecting Apache Commons Text. Starting with version 1.5 and continuing through 1.9, the set of default Lookup instances included interpolators that could result in arbitrary code execution. The Apache Software Foundation has released Apache Commons Text version 1.10.0, which disables the problematic interpolators by default.

PSIRT Statement

Carrier Product Cybersecurity has not identified any offerings may be impacted by the Text4Shell vulnerability. Should there be a determination that any 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 Software Foundation:

https://blogs.apache.org/security/entry/cve-2022-42889

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
November 4, 2022	December 16, 2022