PRODUCT SECURITY ADVISORY

November 30, 2022

PSIRT Record Number
CARR-PSA-009-1122

Overview

CVE-2022-37026 was published as a Client Authentication Bypass in specific Erlang/OTP versions under certain client-certification situations for SSL, TLS, DTLS.

- Erlang/OTP versions before 23.3.4.15, 24.x before 24.3.4.2, and 25.x before 25.0.2 are affected.

Users of LenelS2's OnGuard platform are exposed to Erlang/OTP through the installation/use of RabbitMQ, a third-party component within the OnGuard platform that supports communications.

- OnGuard versions 7.5, 7.6, 8.0, and 8.1 utilize affected versions of Erlang/OTP.

PSIRT Statement

OnGuard Version 7.6 Update 4 has just been released with non-vulnerable versions of Erlang/RabbitMQ.

Until additional remediation is supported, the vulnerability can be mitigated with a configuration file modification by changing the RabbitMQ advanced.config file from using

“verify_peer” to “verify_none”, using the steps below:

1. On the identified Message Broker Service Host (See OnGuard System Options dialog)
2. Use Windows Services and Stop LS Message Broker service
3. Navigate to C:\ProgramData\Lnl\RabbitMQ and edit the advanced.config file as an administrator.
    a. Within the file, update the two lines…

        {verify,verify_peer},

        {fail_if_no_peer_cert,true}

    b. To a single line with the value…

        {verify,verify_none}
4. Save the updated file and start LS Message Broker service.

Once support for the newer versions of RabbitMQ (Erlang/OTP) are confirmed an additional notification memo will be sent to provide closure of the issue.

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 30, 2022	November 30, 2022