



VxWorks TCP Predictability Vulnerability

UR Product Line

Security Notice

Date: 6 April 2017
Last updated: 8 March 2018
ID: DESN-2017-001-5

Classification: Confidential
CVSS: (AV:N/AC:M/Au:N/C:P/I:N/A:P)
ICS-CERT Advisory: ICSA-15-169-01
CVE Identifier: CVE-2015-3963

Overview

A vulnerability has been identified in the GE Vernova Universal Relay (UR) product line that could result in an attacker spoofing or disrupting TCP communications. The vulnerability exists within the third-party VxWorks operating system and affects all versions of the UR family of protection and control products.

This issue has the potential to be exploited remotely through network interfaces that utilize the TCP protocol. The UR supports the DNP3 server, MODBUS/TCP server, IEC 60870-5-104 server, IEC 61850 MMS server, HTTP server, and Synchrophasors on the TCP layer. The associated TCP connections can be disrupted with the client if this vulnerability is exploited.

Vulnerability Details

Wind River Systems, the maker of the VxWorks operating system, released a security advisory on March 9th, 2015 including disclosure that its network stack was susceptible to a TCP sequence number prediction attack. This type of vulnerability may be exploited against established TCP sessions to disrupt the connection by injecting counterfeit packets with valid TCP sequence numbers. In more complex scenarios, it can be used to impersonate the device that originally established the connection.

The UR family of products includes VxWorks with a version less than 6.8.3, which Wind River has disclosed is susceptible to this vulnerability. In response, GE Vernova updated firmware to resolve this issue and upgrade the included version of VxWorks to 6.8.3.

Mitigation

GE Vernova recommends that users update their UR devices to version 6.06, 7.26, 7.32, or 7.4x or later to resolve this issue. It is recommended that users evaluate their current risk and implement appropriate network security mitigation measures as follows:

- Implement a bump-in-the-wire solution that can provide secure communication between endpoints, which can enhance security
- Effectively segment networks and implement demilitarized zones (DMZs) with properly configured firewalls to selectively control and monitor traffic passed between zones

-
- Minimize network exposure for all control system devices and/or systems, and ensure that they are not accessible from the Internet
 - Locate control system networks and remote devices behind firewalls, and isolate them from the business network

GE Vernova Product Security Incident Response Team (PSIRT)

GE Vernova is committed to helping ensure the security of its customer base. To report product security issues and to request security support, contact the PSIRT at www.gevernova.com/security or GEV.PSIRT@gevernova.com.

Product Support

GE Vernova Grid Solutions is committed to the continued support of the UR product line. We appreciate your business and look forward to continuing to grow our relationship.

If you need help with any aspect of your GE Vernova Grid Solutions product, use the following options:

Search Technical Support

The GE Vernova Grid Solutions Web site provides fast access to technical information, such as manuals, release notes, and knowledge base topics. Visit us on the Web at: <https://www.gevernova.com/grid-solution>

Contact Customer Service

The GE Vernova Grid Solutions Customer Service Center is open 24 hours a day, seven days a week for you to talk directly to a GE Vernova representative.

In the U.S. and Canada, call toll-free: 1 800 547 8629

International customers please call: + 1 905 294 6222

Or e-mail to: ge4service@gevernova.com