



GE VERNOVA

UR Family

Triangle MicroWorks DNP3 Outstation Libraries Vulnerability

Security Notice

Publication Number: GET-20091

Copyright © 2026 GE Vernova

Initial Release: 25 May 2020

ID: UR-2020-0001

ICS-CERT Advisory: ICSA-20-105-02

This document outlines vulnerabilities in the GE Vernova Universal Relay (UR) family of products with the integrated Triangle MicroWorks (TMW) DNP3 Outstation Libraries.

Applicable products: B30, B90, C30, C60, C70, D30, D60, F35, F60, G30, G60, L30, L60, L90, M60, N60, T35,

T60 Impacted versions: 6.06, 7.21 to 8.01

Action: Upgrade to version 8.02 or later

Introduction

After notification of a TMW DNP3 Outstation Libraries vulnerability that was released by ICS-CERT on 14 April 2020, GE Vernova evaluated the UR products utilizing TMW DNP3 libraries. UR products with firmware releases 6.06 and 7.21 to 8.01 are impacted with the disclosed vulnerability.

TMW has provided a fix for this vulnerability to product manufacturers whose implementation of DNP3.0 incorporates the TMW Libraries. GE Vernova is working to provide the fix for this vulnerability in the UR product family. GE Vernova is committed to security and will notify impacted customers as appropriate when affected UR revisions are upgraded to incorporate the solution to the DNP3.0.

Vulnerability

ICS-CERT released security advisory [ICSA-20-105-02](#) on 14 April 2020 regarding a TMW DNP3 Outstation Library vulnerability.

Vulnerability: Stacked-based Buffer Overflow - Critical

A specially crafted message can cause a stack-based buffer overflow. Authentication is not required to exploit this vulnerability. The vulnerability affects TMW libraries 3.16.00 through 3.25.01.

Action

GE Vernova strongly recommends that users with impacted firmware versions update their UR devices to UR firmware version 8.02 or greater to resolve this vulnerability. New minor revisions of released firmware also will include a vulnerability patch.

GE Vernova recommends that users evaluate their current risk and take defensive measures to minimize the risk of exploitation of this vulnerability. Suggested security practices are as follows:

- 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
- When remote access is required, use secure methods, such as Virtual Private Networks (VPNs), recognizing that VPNs can have vulnerabilities and should be updated to the most current version available. Also recognize that VPN is only as secure as the connected devices.
- Analyze security events to detect early any unexpected traffic/communication

Implementing the mitigation measures listed above helps to reduce the risk of exploitation until the UR firmware is upgraded to a version with the fix for the vulnerability.

GE Vernova recommends that impacted organizations perform proper impact analysis and risk assessment prior to deploying defensive measures. Note that the mitigation measures listed here do not ensure complete security.

Reporting

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 GE Vernova Product Security Response Team (PSIRT) at <http://www.gevernova.com/security> or GEV.PSIRT@gevernova.com.

For further assistance

For product support, contact the information and call center as follows:

GE Vernova
650 Markland Street
Markham, Ontario
Canada L6C 0M1
Worldwide telephone: +1 905 927 7070
Europe/Middle East/Africa telephone: +34 94 485 88 54 North
America toll-free: 1 800 547 8629
Fax: +1 905 927 5098
Worldwide e-mail: multilin.tech@gevernova.com
Europe e-mail: multilin.tech.euro@gevernova.com
Website: <https://www.gevernova.com/grid-solutions/multilin>