



GE VERNOVA

UR Family **DNP3 Implementation Vulnerability**

Security Notice

Publication Number: GET-20046A

Copyright © 2026 GE Vernova

Initial Release: 9 August 2016

ID: DESN-2015-001-1

ICS-CERT Advisory:

ICSA-13-291-01B

Updated: 25 April 2018

CVSS: (AV:N/AC:M/Au:N/C:P/I:N/A:P)

CVE Identifier: CVE-2013-2811b

This document outlines a Distributed Network Protocol (DNP) vulnerability in the GE Vernova Universal Relay (UR) family of products.

Applicable to products: B30, B90, C30, C60, C70, D30, D60, F35, F60, G30, G60, L30, L60, L90, M60, N60, T35, T60

Impacted versions: Up to 6.05, 7.00 to 7.20

Action: Upgrade to version 6.06, 7.21 or later

Introduction

A vulnerability has been identified in the UR product line that can result in denial of service to the DNP slave functionality on the UR, requiring a power cycle to the relay to recover. This vulnerability is accessible via serial or Internet protocol (IP) based networks and affects the UR firmware versions identified.

Network interfaces that utilize the Transmission Control Protocol (TCP) can be exploited remotely, but serial access is not exploitable remotely and local access to the serial based outstation is required.

Vulnerability

The Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) of the United States released a security advisory ICSA-13-291-01B on 9 April 2014 regarding a DNP3 implementation vulnerability that the outstation/slave can be sent into an infinite loop or Denial of Service condition by sending a specially crafted packet from a master station that can result in the DNP slave functionality on the UR locking up and requiring a power cycle to the relay to recover from this condition.

Action

GE Vernova recommends that all users update their UR devices to version 6.06 or 7.21 or later to resolve this issue.

It is recommended that users evaluate their current risk and implement appropriate network security mitigation measures 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 a Virtual Private Network (VPN), recognizing that VPN is only as secure as the connected devices

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>