

UR Family

Wind River VxWorks Debug Service Enabled by Default

Security Notice

Publication Number: GET-20047A

Copyright © 2026 GE Vernova

Initial Release: 9 August 2016

ID: DESN-2015-001-1

ICS-CERT Advisory: ICSA-10-214-01

Updated: 5 June 2018

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

A:P) CVE Identifier: CVE-2010-2965

This document outlines a vulnerability in the GE Vernova Universal Relay (UR) family of products with the integrated VxWorks debug service enabled by default.

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

Impacted versions: All to 5.47, 5.80 to 5.82, 5.90 to 5.91, 6.00 to 6.01

Action: Upgrade to version 6.06, 7.26, 7.32, 7.40 or greater

Introduction

An insecure default configuration has been identified in the UR product line that can result in access to debug information and code execution. UR products with firmware releases prior to 5.48, 5.80 to 5.82, 5.90 to 5.91, 6.00 to 6.01 are susceptible to this vulnerability.

This issue has the potential to be exploited remotely through Ethernet network interfaces that utilize User Datagram Protocol (UDP) port 17185. The UR products based on VxWorks have the Wind River Debug (WDB) target agent debug service enabled by default. An adversary can use the debug service to compromise the device.

In UR versions 5.48, 5.49, 5.83, 5.92, 6.02 to 6.05, 7.00 to 7.25, and 7.31, the VxWorks debug port is password-protected with two factory-service passwords.

Vulnerability

ICS-CERT released a security advisory ICSA-10-214-01 on June 2nd, 2014 regarding Wind River Systems VxWorks debug service enabled by default finding that some products based on VxWorks have the WDB

target agent debug service enabled by default. This service provides read/write access to the device's memory and allows functions to be called. An adversary can use the debug service to compromise the device.

Action

GE Vernova recommends that users with impacted versions update their UR devices to UR firmware version 6.06, 7.26, 7.32, 7.40 or greater to resolve this issue. The VxWorks debug port is disabled by default in these releases.

Otherwise, GE Vernova recommends that users evaluate their current risk and implement appropriate network security mitigation measures as follows:

- Implement appropriate firewall rules to restrict access to the debug service (17185/UDP) to only trusted sources until a corresponding minor release of your locked firmware revision can be applied. That is, GE Vernova recommends that customers close UDP port 17185 in the firewall.
- For versions 5.5x, 5.6x, and 5.7x, GE Vernova recommends closing the port in the firewall

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>