GE VERNOVA

Grid Solutions

Grid Automation - Protection Automation Control

# Security Notice

Date: 22 January **2026** Distribution: **Public** Reference: **GES-2025-05**

## Affected product family "UR"

# UR IED & EnerVista UR Setup: vulnerabilities fixed in version 8.70

## References

| | |
|---|---|
| Publication number | GES-2025-005 |
| Release date | 22 January 2026 |

## Overview

The Universal Relay (UR) family of protection and control products are developed based on the Secure Development Life Cycle Process. As per the process, we ensure remediation of any weakness found internally, as well as the ones reported to our PSIRT (Product Security Incident Response Team). This document describes reported vulnerabilities corrected in version 8.70 along with impacted areas and recommended actions.

The UR firmware is affected by the underlying Wind River VxWorks Real-Time Operating System (RTOS). Version 8.70 addresses two such vulnerabilities by applying patches provided by Wind River. Additionally, we have corrected the IED configuration software (EnerVista UR Setup) based on two vulnerabilities brought to our attention by DRAGOS vulnerability research.

GE Vernova thanks Reid Wightman, of DRAGOS for responsibly disclosing vulnerabilities in our product to our PSIRT team and their engagement with GE Vernova on such matters.

At the time of publication of this document, there have been no reported cybersecurity attacks that exploited the vulnerabilities described in this document. GE Vernova is addressing these vulnerabilities as part of its commitment to improve security in its products.

## Background

The UR family of advanced protection and control relays provides an integrated platform that delivers leading edge protection, control, monitoring, and metering solutions for critical power system applications. The UR platform supports proven protection algorithms, expandable I/O, integrated monitoring, and high accuracy metering capabilities with the latest in communications technologies. The UR family of devices provides the situational awareness needed for a reliable, secure, and efficient modern grid.

Copyright 2026, GE Vernova. All Rights Reserved.

UR relays are digital devices designed to be installed and operated in a utility and industrial environment and connected to secure private networks.

EnerVista UR Setup is a software program developed by GE Vernova, which simplifies every aspect of connecting and using the UR device. EnerVista UR Setup is a user-friendly device configuration tool that is compatible with all UR relay applications. It also allows the user to monitor the status of the protected asset, maintain the UR device, conveniently view COMTRADE & event records to carry out postmortem event analysis and ensure proper protection system operation. This software is license-free and the latest version is always published on our website.

## Vulnerability Details

We confirm that the following Common Vulnerabilities and Exposures (CVEs) are applicable to the UR and needed a patch from Wind River.

1. CVE-2020-10664: The IGMP (Internet Group Management Protocol) component in VxWorks 6.8.3 IPNET CVE patches created in 2019 has a NULL Pointer Dereference.
   (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H score: 7.5 High)
   Affected products/versions:

| Products | Affected versions |
|---|---|
| UR firmware with IEC61850 order codes | UR FW version 7.43 to 7.46, 7.64 to 7.66, 7.82 and higher up to version 8.62 |

   The IGMP is used by UR IEDs in Routable GOOSE (R-GOOSE) applications for managing the membership of the UR relays in a specific multicast group.

   Due to this CVE, the R-GOOSE subscription capability was removed in EnerVista Setup version 8.6x.

   If the R-GOOSE feature is not used by a UR user, this vulnerability will not impact their IED.

   In version 8.70, the CVE is fixed by applying a patch provided by WindRiver and the R-GOOSE subscription capability was restored in EnerVista Setup version 8.7x.

2. CVE-2020-28895: Wind River VxWorks memory allocator issue.
   (CVSS:3.1:: AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:L score: 7.3)
   Affected products/versions:

| Products | Affected versions |
|---|---|
| UR IED | Firmware versions 7.00 to 8.62 |

   In Wind River VxWorks, the memory allocator has a possible overflow when calculating the memory block's size to be allocated by calloc(). As a result, the actual memory allocated is smaller than the buffer size specified by the arguments, leading to memory corruption.

   Our development team has identified no feasible exploit vectors, but the vulnerability was fixed as a preventative measure.

3. EnerVista UR Setup Software: zip-slip vulnerability.
   (CVSS: 3.1 :: AV:P/AC:L/PR:H/UI:N/S:U/C:N/I:L/A:L score: 2.9)
   Affected products/versions:

Copyright 2026, GE Vernova. All Rights Reserved.

| Products | Affected versions |
|---|---|
| EnerVista UR Setup Software | All versions prior to UR Setup version 8.70 |

The EnerVista UR Setup software helps the user to connect to the UR IED over a SSH encrypted channel. For firmware upgrades, EnerVista UR Setup extracts the firmware files from SFD file selected by user and sends these extracted files to the IED device.

EnerVista UR Setup versions earlier than 8.70, mishandle the processing of the SFD file content by addressing the extracted files using a relative path. This flaw enables attackers to manipulate and send incorrect files to the device.

As a corrective action, EnerVista UR Setup 8.70 extracts the firmware SFD file and validates the files before sending it to the device, by picking it up from the explicit location from where it was unpacked.

UR IEDs version 8.60 and higher validate the firmware file before upgrading, hence the impact of this weakness is considered to be low.

4. EnerVista UR Setup: dll hijacking vulnerability.

(CVSS: 3.1: AV:P/AC:L/PR:H/UI:N/S:U/C:L/I:H/A:N score: 4.6)

Affected products/versions:

| Products | Affected versions |
|---|---|
| EnerVista UR Setup Software | All earlier versions prior to UR Setup software version 8.70 |

The EnerVista URPC installation software versions prior to 8.70, used an incorrect method of loading the DLL (dynamic Link Library) file by referencing it relative to the location of the installation folder. If the system in which the software is installed gets compromised, an attacker could exploit this weakness and replace the legitimate DLL with a malicious file.

The EnerVista UR Setup software installation has been upgraded to address this vulnerability.

## Resolution

We strongly recommend that users with impacted firmware versions update their UR devices to UR firmware version 8.70, released in November 2025, to resolve these vulnerabilities. We also recommend upgrading the EnerVista UR Setup configuration tool to version 8.70 or greater.

Enervista UR Setup software is backward compatible, users can upgrade it to version 8.70, independently of upgrading their UR IED to FW v870.

## Workaround / Mitigation

As a workaround, GE Vernova recommends having secure infrastructure in place, which can protect the system. We also recommend that customers protect their digital devices using a defense-in-depth strategy. This includes, but is not limited to, placing digital devices inside the control system network security perimeter, access controls, robust network monitoring (such as Intrusion Detection System) and other mitigation techniques in place. Please refer to the product secure deployment guide.

Copyright 2026, GE Vernova. All Rights Reserved.

It is essential for organizations to prioritize cybersecurity measures, including regular vulnerability assessments and prompt application of security patches.

--- -- ---

## GE Product Security Incident Response Team (PSIRT)

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

## For Product Support

For questions or further product support, please contact the GE support team using the following contact details:

| Region | E-mail | Telephone |
|---|---|---|
| Global Contact Centre | ga.support@gevernova.com | +44 1785 250070 |
| Central, East Asia, Pacific | ga.supportCEAP@gevernova.com | +61 414 730 964 |
| India | ga.supportIND@gevernova.com | +91 44 2264 8000 |
| Middle East, North Africa, Turkey | ga.supportMENAT@gevernova.com | +971 4 375 6950 |
| Europe, Russia, CIS, Sub-Saharan Africa | ga.supportERCIS@gevernova.com | +34 94 485 8854 |
| North America | ga.supportNAM@gevernova.com | +1 877 605 6777 |
| Latin America | ga.supportLAM@gevernova.com | +55 48 2108 0300 |

## Document revision history

| Version | Date | Change Description |
|---|---|---|
| GES-2025-005 | 14 DEC 2025 | Initial release |
| GES-2025-005 | 22 Jan 2026 | Updated contacts and minor modifications |

## Disclaimer:

Unless the product is under a GE Vernova service contract, GE Vernova assumes no responsibility or liability for the content of Security Notices or for making Security Notices available to customer. Implementing Security Notices as well as performing updates/upgrades to software/firmware is solely the responsibility of the customer.

Copyright 2026, GE Vernova. All Rights Reserved.