



UR Product Family

UR Software Vulnerabilities & fixes

Security Notice

Copyright © 2026 GE Vernova

Security: GE Vernova Proprietary Information – Class III (Confidential)

Release Date: 24 February 2023

Ref ID: GE Vernova GES-2023-001

CVSS: Multiple (refer section "Vulnerability details")

CVE Identifier: Multiple (refer section "Vulnerability details")

Overview

The UR family of relays are developed using the Secure Development Life Cycle Process. As per the process, we regularly assess our product internally to ensure there are no weaknesses, and we thoroughly analyze reported vulnerability-related queries. In accordance with these assessments, we found three vulnerabilities for the UR platform, for which we have taken appropriate action with latest software release. This document describes these vulnerabilities and the affected areas. It further recommends actions that UR users can follow.

At the time of this advisory publication, the above security vulnerabilities have not been exploited. We are addressing these vulnerabilities as part of our ongoing commitment to improve security in our products.

Background

The UR family of advanced protection and control relays provides a single 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 with the latest communications technology. <https://www.gevernova.com/grid-solutions/multilin>

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

Vulnerability Details

The three vulnerabilities, which are fixed in UR version 8.40, are listed here. The table provides details about the product variant and affected versions.

Wind River VxWorks Vulnerability:

A flaw in the VxWorks memory allocator may enable a buffer overflow attack. As the UR does not allow arbitrary inputs, such an attack is highly unlikely to succeed.

Vulnerability details: CVE-2020-35198

- CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H (Base score: 9.8)

Affected products/versions

Products	Versions
UR Family: B30, B90, C30, C60, C70, C95, D30, D60, F35, F60, G30, G60, L30, L60, L90, M60, N60, T35, T60	All firmware versions from FW 7.00 onwards through version 8.30.

The zlib library component

The zlib library component used in the affected UR firmware versions is affected by the two CVEs listed below. This component is used in firmware to compress and decompress the IEC61850 CID file. As the CID file is created by Enervista software, it is highly unlikely that an attempt to exploit these vulnerabilities will succeed.

Vulnerability details: CVE-2016-9840

- CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H (Base score : 8.8)

Vulnerability details: CVE-2016-9841

- CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H (Base score: 9.8)

Affected products/versions

Products	Versions
UR Family: B30, B90, C30, C60, C70, C95, D30, D60, F35, F60, G30, G60, L30, L60, L90, M60, N60, T35, T60	All firmware versions from FW 7.30 onwards through version 8.30, only with IEC61850 software option

TFTP UDP PORT issue:

The UR family of relays supports the Trivial File Transfer Protocol (TFTP) to transfer files over a network at a port configured through the setting **TFTP MAIN UDP PORT NUMBER**. By default, the port number is configured to 69. Since firmware version 7.00 the range of this setting is 0 to 65535, with the value of 0 closing the TFTP port after an additional reboot. It was recommended to configure the TFTP MAIN UDP port to 0 when the TFTP service is not needed.

We are confirming the erroneous behavior of the UR platform when the "TFTP MAIN UDP PORT NUMBER" setting is configured to 0. When the TFTP MAIN UDP port number is configured to 0, after the device is rebooted, a random port number is opened for the TFTP protocol and the TFTP server can be accessed using that random port.

Please note: The UR relays support only READ operations over TFTP (when enabled). The "put" function is not supported for security reasons. Only the **get** command is supported.

Vulnerability details

- Information Exposure Through Directory Listing CWE-548
- Information Exposure Through Log Files CWE-532

- Information Exposure CWE-200
- CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:L/I:N/A:N (Base score 5.6)

Affected products/versions:

Products	Versions
UR Family: B30, B90, C30, C60, C70, C95, D30, D60, F35, F60, G30, G60, L30, L60, L90, M60, N60, T35, T60	All firmware versions from FW 7.00 onwards through version 8.30

Actions

We strongly recommend that users with affected firmware versions update their UR devices to UR firmware version 8.40, released in Q4 2022, or greater to resolve this vulnerability. We will work with customers on minor releases for affected UR firmware.

As a workaround for TFTP related issue, we recommend that you either configure the firewall to block all TFTP traffic to your relays or configure the TFTP UDP port to a non-zero value and block traffic to only that port using a firewall.

We also recommend that you secure the physical access to the UR relays and protect the digital devices using a **defense-in-depth** strategy. This includes, but is not limited to:

- Placing all digital devices inside the control system network security perimeter
- Deploying, and maintaining access controls, monitoring and intrusion detection
- Conducting security awareness training on security policies, network segmentation and firewalls, strong and active password management, data encryption, antivirus, and other mitigating applicable technologies.

Please refer to the *UR family secure deployment guide* for secure configuration of UR relays.

Product support

For help with any aspect of your GE Vernova product, visit our website to contact our support team, 24/7, as follows:

Region	E-mail	Telephone
Global Contact Centre	ga.support@gevernova.com	+44 1785 250070
Central and East Asia and Pacific	ga.supportCEAP@gevernova.com	+61 414 730 964
India	ga.supportIND@gevernova.com	+91 44 22648000
Middle East, North Africa and Turkey	ga.supportMENAT@gevernova.com	+971 42929467
Europe, Russia, CIS and Sub-Saharan Africa	ga.supportERCIS@gevernova.com	+34 94 4858854
North America	ga.supportNAM@gevernova.com	+1 877 605 6777
Latin America	ga.supportLAM@gevernova.com	+55 11 36187308

