



UR Product Family

UR vulnerabilities resolved in 8.10 and Subsequent releases

Security Notice

Publication Number: GES-2021-004 v2

Copyright © 2026 GE Vernova

Security: GE Vernova Proprietary Information

Document release Date: 3 February 2021

CVSS: Multiple (refer section “Vulnerability details”)

CVE Identifier: Multiple (refer section “Vulnerability details”)

Overview

This document describes vulnerabilities initially corrected in version 8.10. The version 8.10 addresses several weaknesses, some of which have been brought to our attention by SCADA-X, CyTRICS, Verve Industrial and VuMetric. The disclosed vulnerabilities impact all firmware versions prior to 8.10. Additional vulnerabilities related to SSH impact firmware version 7.4x to 8.0x. For detailed description of these vulnerabilities and affected versions, please refer to section “Vulnerability details”. Major firmware versions scheduled for release after version 8.10 (e.g., version 8.20) will include these changes. Minor firmware versions released after 8.10 (e.g., version 7.28) will provide the ability to mitigate the vulnerabilities mentioned in this report, through methods described in each section.

This document provides information on the nature of these vulnerabilities as well as recommends mitigation measures.

GE Vernova thanks SCADA-X, CyTRICS, Verve Industrial and VuMetric for responsibly disclosing vulnerabilities in our product and their engagement with GE Vernova on such matters.

At the time of issuing this document, there are no reported cybersecurity attacks which exploited the vulnerabilities in this document. GE Vernova is addressing these vulnerabilities as part of its commitment to improve security in our products.

Background

The UR family of advanced protection and control relays provides one integrated platform that delivers leading edge protection, control, monitoring and metering solutions for critical power system applications. 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.

Vulnerability details

This section details vulnerabilities initially fixed in firmware version 8.10. For each vulnerability we provide description, potential impact, and mitigation measures.

Vulnerabilities related to SSH support

UR family of products with CyberSentry option supports MODBUS over SSH as well as SFTP for communication with the IED. Impacted UR products and firmware versions are mentioned in following table:

Impacted Products	Impacted 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 7.4x to 8.0x with CyberSentry™ software option

Below is the list of applicable vulnerabilities which are initially resolved in firmware version 8.1x.

SSH Weak encryption and MAC Algorithms:

Prior to UR firmware version 8.1x, UR supported various encryption and MAC algorithms for SSH communication, some of which are weak.

Vulnerability scored: Weak encryption algorithms: CVE-2016-2183: High and CVE-2013-2566: Medium
Weak MAC algorithms (MD5 and 96 bit): Low

Remediation: From UR firmware version 8.1x onwards, DES, 3DES, ARCFOUR algorithms are removed.
MAC algorithms with MD5 and 96- bit algorithms are removed

Session Key Retrieval and Insertion Attack:

Prior to firmware version 7.4x, UR supported only SSHv2. Starting from firmware version 7.4x, UR added support to SSHv1. SSHv1 has known vulnerabilities (SSH Protocol Session Key Retrieval and Insertion attack).

Vulnerability scored: Session Key Retrieval - High
Insertion Attack: CVE-1999-1085 - Medium

Remediation: From UR firmware version 8.1x onwards, SSHv1 support is removed.

Mitigation for SSH vulnerabilities:

GE Vernova strongly recommends that users with impacted firmware versions update their UR devices to UR firmware version.

8.1x, or newer to address these vulnerabilities. This includes minor firmware releases.

UR has discontinued support to SSHv1 from firmware version 8.1x onwards.

GE Vernova recommends the use of SSH clients that support secure algorithms when connecting to the UR IED.

Web Server Vulnerabilities

UR family of products supports webserver over HTTP for accessing read-only information from the IED. Impacted UR products and firmware versions are mentioned in following table:

Affected Products	Affected 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 prior to version 8.1x

Below is the list of applicable vulnerabilities which are initially resolved in firmware version 8.1x.

Information Exposure:

Web server interface is supported on UR over HTTP protocol. It allows sensitive information exposure without authentication. The applicable weaknesses are CWE-200, CWE-532 and CWE-548.

Vulnerability score: Medium

Remediation: Starting with UR firmware version 8.1x, the “CyberSentry” option limits the information available on UR web server. Sensitive information is no longer available on web server. Such information is made available only over SFTP and can be retrieved using UR Setup based on authorization.

Improper Neutralization of Script-Related HTML Tags in a Web Page and Lack of HTML Encoding on User Supplied Strings

UR supports web interface with read-only access. The device fails to properly validate user input, making it possible to perform XSS attacks, which may be used to send a malicious script. Also, UR Firmware web server does not perform HTML encoding of user-supplied strings.

Vulnerability score: Medium

Remediation: Starting with UR firmware version 8.1x certain special characters that could lead to XSS attacks are not supported anymore.

Temporary HTTP Denial of Service via Unsupported HTML Verbs

UR Firmware web server task does not properly handle receipt of unsupported HTTP verbs, resulting in the web server becoming temporarily unresponsive after receiving a series of unsupported HTTP requests. When unresponsive, the web server is inaccessible. By itself, this is not particularly significant as the relay remains effective in all other functionality and communication channels.

Vulnerability score: Medium

Remediation: Starting from UR firmware version 8.1x, the UR IED disconnects the client for any other http request, but “GET”.

Mitigation for Webserver vulnerabilities:

GE Vernova recommends that UR IED users upgrade to firmware version 8.1x or newer with CyberSentry security option to fix these vulnerabilities.

As workaround, UR IED users can evaluate the usage of the web-interface and, whenever possible, and disable it (by configuring HTTP protocol port to “0”). When HTTP protocol is disabled, then it may impact UR Setup features: Quick Connect and Discover.

Protection from un-intended firmware upload

Impacted UR products and firmware versions are mentioned in following table:

Affected Products	Affected 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 prior to version 8.1x with basic security option

UR IED supports upgrading firmware using UR Setup configuration tool – Enervista UR Setup. This UR Setup tool validates the authenticity and integrity of firmware file before uploading the UR IED. It was brought to our notice that there is possibility that illegitimate user can upgrade firmware without appropriate privileges. The weakness is assessed, and mitigation is implemented in firmware version 8.10.

Vulnerability score: Medium

Remediation: Firmware version 8.1x onwards, UR supports “Firmware lock” setting in both basic and CyberSentry UR IED. This setting is “Enabled” by default. That means, firmware upgrade is not allowed unless user with appropriate privileges changes the configuration of this setting.

NOTE: For UR with CyberSentry security option, firmware version 7.2x to 8.0x, user can protect against this un-intended firmware upgrade using the setting “Lock Relay” available in Settings\Product setup\Security settings screen. This setting is by default “Disabled”, but it can be enabled by a user with “Administrator” privileges.

Mitigation: GE Vernova recommends that UR IED basic security users upgrade to firmware version 8.1x or newer to fix this weakness. Minor firmware releases cannot include fixes for this vulnerability, customer can choose from upgrading their devices with CyberSentry™ software option or implementing defense-in-depth practices.

Provision to disable Factory Mode

Impacted UR products and firmware versions are mentioned in following table:

Affected Products	Affected 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 prior to 8.1x without CyberSentry™ security option

UR devices without CyberSentry™ software option do not allow the disabling of the “Factory Mode”, which is used for servicing the IED by a “Factory” user.

Vulnerability score: High

Remediation: Firmware version 8.1x onwards, UR added a “Factory service mode” setting in devices without CyberSentry™ security option. This setting is “Disabled” by default. Only user with “Settings” level access can

enable the factory service mode. That means, “Factory” user can only gain access when user with appropriate privileges changes the configuration of this setting.

Firmware version 7.0x onwards, with CyberSentry™ option already includes a setting “Factory service mode” that allows the disabling of the factory mode. By default, this setting is “Disabled” and can be “Enabled” only by user with “Administrator” privileges.

Some enhancements are made as part of CyberSentry™ as well as basic security variants of UR IED in UR 8.1x. When privileged user enables the factory service mode, a security event gets logged in the IED. Also, the TROUBLE LED stays ON for the duration of Factory mode being enabled.

Mitigation: GE Vernova recommends that UR IED without CyberSentry™ security option are upgraded to firmware version 8.1x or newer to fix this weakness. Minor firmware releases cannot include fixes for this vulnerability, customer can choose from upgrading their devices with CyberSentry™ software option or implementing defense-in-depth practices. Additionally, as part of defense-in-depth practices, it is recommended that users secure physical access to the UR IED front panel because the factory user can get logged in only from front the front panel.

Access to “Last-key pressed” register

Impacted UR products and firmware versions are mentioned in following table:

Affected Products	Affected 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 prior to 8.1x without CyberSentry™ security option

GE Vernova shares the UR MODBUS memory map as part of the product communications guide. GE Vernova was made aware that “Last-key pressed” MODBUS register can be used to gain unauthorized information.

Vulnerability score: High

Remediation: From UR firmware version 8.1x onwards, the “Last key pressed” MODBUS register is not accessible anymore.

Mitigation GE Vernova strongly recommends that users with impacted firmware versions update their UR devices to UR firmware version 8.10, or newer to resolve this vulnerability. This fix will be part of UR minor firmware releases (e.g. 7.28). Customer who are not able to update firmware can opt for upgrading their devices with CyberSentry™ software option.

Weakness in UR Bootloader binary

Impacted UR bootloader binary versions are mentioned in following table:

Affected Products	Affected Versions
UR Family (B30, B90, C30, C60, C70, D30, D60, F35, F60, G30, G60, L30, L60, L90, M60, N60, T35, T60)	All bootloader versions prior to 7.03/7.04

UR bootloader binary version 7.00, 7.01 and 7.02 included unused hardcoded credentials. Additionally, a user with physical access to the UR IED can interrupt the boot sequence by rebooting the UR.

Vulnerability score: Medium

Remediation: From bootloader binary 7.03 onwards, the unused hardcoded line is removed.

Mitigation GE strongly recommends upgrading the Bootloader binary to 7.03 or higher. As an alternative, as part of defense-in-depth practices, it is recommended that users secure physical access to the UR IED.

Generic recommendation:

GE Vernova recommends that UR IED be protected using defense-in-depth practices. This includes, but is not limited to, placing UR IED inside the control system network security perimeter, and having access controls, monitoring (such as an Intrusion Detection System), and other mitigating technologies in place.

Please refer UR Deployment guide for secure configuration of UR IED and system.

Product support

For help with any aspect of your GE Vernova Grid Solutions product, please contact our support team, 24/7,

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

GE Vernova Product Security Incident Response Team (PSIRT)

GE Vernova 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@ge.com.

Document revision history

Version	Date	Change description
GES-2021-004	3 Feb 2021	Initial release
GES-2021-004 v2	25 March 2021	Review to mention future and quality firmware releases