



UR / UR^{Plus} Families

Cryptographic Algorithm Weakness

Security Notice

Publication Number: GET-20073
Copyright © 2026 GE Vernova

Initial Release: 5 May 2017
ID: UR-2017-0001
ICS-CERT Advisory: ICSA-17-117-01

Updated: 28 August 2018 CVE
Identifier: CVE-2017-7905

This document outlines a vulnerability and mitigation for the GE Vernova Universal Relay (UR) and UR^{Plus} families of products.

Applicable to products: B30, B90, C30, C60, C70, D30, D60, F35, F60, G30, G60, L30, L60, L90, M60, N60, T35, T60, B95^{Plus}, C90^{Plus}, D90^{Plus}

Introduction

GE Vernova determined that the algorithm used to encrypt passwords in the UR/UR^{Plus} products has a weakness that can allow an unauthorized actor to obtain the cipher text of the user-configured password and decrypt it. Researchers from New York University (NYU) made a similar determination regarding the GE Vernova SR750 Feeder Management Relay (see Security Advisory (SR-2017-00001)).

Vulnerability

In a confidential report to GE Vernova regarding the SR750 Feeder Management Relay, NYU security researchers identified that it is possible to decrypt the cipher text of the user-configurable password from the relay. GE Vernova determined that the UR/UR^{Plus} products use a similar mechanism. In specific versions, access to the encrypted password is possible through the UR/UR^{Plus} front panel or remotely through Modbus or the device webpage. With access to the password, the device settings can be modified. The affected cipher text is not accessible via any physical port configured to use DNP3.

There have been no known public exploits of this issue.

The vulnerability is categorized by OWASP as both CWE-261 (Weak Cryptography for Passwords) and CWE-329 (Not Using a Random IV with CBC Mode). Where users have multiple devices that share a common password, decrypting the password from one device also gives the password for those devices.

To address the vulnerability, GE Vernova removed the ability to obtain the password cipher text in the UR when changes were made to the password reset functionality in version 7.x and later, as well as certain firmware releases below 7.0. Similar changes were made for UR^{Plus} releases.

Action

For UR, GE Vernova recommends that users update to firmware versions 7.x and above that include the CyberSentry option designed to meet NERC CIP requirements or to an updated firmware version listed in the table.

For UR^{Plus}, GE Vernova recommends updating to firmware versions outlined in the table.

The revised versions remove access to the cipher password text from the front panel, Modbus, and the device webpage.

Table 1: Releases affected and upgrades available

Product	Affected releases	Upgrade to
UR	All to 5.48 5.50 to 5.82 5.90, 5.91 6.00, 6.01	5.49 5.83 and subsequent minor releases 5.92 and subsequent minor releases 6.02 and subsequent minor releases 7.00 and later
C90 ^{Plus} , D90 ^{Plus}	All to 1.85 1.90, 1.91	1.86 and subsequent minor releases 1.92 and subsequent minor releases
B95 ^{Plus}	All to 1.02	1.03 and subsequent minor releases

For UR, GE Vernova recommends that users update to firmware versions 7.x and above that include the CyberSentry option or to an updated firmware revision listed in the table. CyberSentry adds the following security features:

- Encryption of communication
- Role-based access
- Password complexity rules
- Remote authentication using RADIUS
- Security events reporting over Syslog

Obtain the firmware from the GE Vernova website. Look in the Support > Software sections.

<https://www.gevernova.com/grid-solutions/multilin>

To reduce the risk of unauthorized access, prior to the installation or availability of the updates, GE Vernova recommends that users restrict the Modbus and webpage access through existing firewalls where available and practical, and that both physical and network security defensive measures are implemented.

While upgrades can be done to a higher firmware version, for example from 5.9 to 6.06, for upgrades to UR firmware version 7.2 or later, for example, be aware of additional hardware and boot firmware requirements. Check release notes or an instructional manual before such an upgrade.

Additional recommendations

Prior to the installation or availability of the updates, evaluate the risk of unauthorized exposure, and where appropriate and practical, restrict the Modbus and webpage access through existing firewall rules. Also implement appropriate physical security as well as network security defensive measures to minimize

risk of exploitation. This includes:

- Utilize physical security to control local access to the device
- Use unique passwords
- Remove passwords when decommissioning devices
- Consider employing an Operations Technology (OT) next generation firewall, such as the Wurldtech OpShield that enforces OT policy at the protocol level, as well as monitors and blocks malicious activity and unintended disruptions
- Use appropriate network segmentation and place the relay within the control system network behind properly configured firewall(s). Protection/Control system devices, such as the UR Family, should not be connected directly to the internet or business networks.
- If remote access into the substation network is required, employ secure methods, such as a Virtual Private Network (VPN), using dual authentication, recognizing that the 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 Product Security Response Team (PSIRT) at <http://www.gevernova.com/security> or GEV.PSIRT@gevernova.com.

Acknowledgements

GE Vernova thanks the NYU security researchers Anastasis Keliris, Charalambos Konstantinou, Marios Sazos, and Dr. Michail (Mihalis) Maniatakos for reporting these issues to GE Vernova, assisting GE Vernova in its investigation, and helping to protect GE Vernova customers.

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>