



Security Notice

Date: **4 October 2024**Distribution: **Public**Reference: **GES-2024-005**

Affected product family “8 Series”

8 Series product IED: Access control for output relay setting modification through HMI

References

Publication number	GES-2024-005
Release date	4 Oct 2024

Overview

The 8 Series family of IEDs are developed using Secure Development Life Cycle Process. As per process, we ensure remediation of weakness found during internal testing as well as we thoroughly analyse reported vulnerabilities. This document describes vulnerability corrected in version 3.02.

Please refer “Vulnerability details” section for impacted version & weakness details.

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

Background

The Multilin™ 8 Series platform of advanced protection and control relays delivers high quality and performance management, protection and control for transformer, generator, motor and feeder applications.

Comprised of the 845 transformer protection relays, 889 generator protection relays, 869 motor protection relays and 850 feeder protection relays, the 8 Series platform features innovative technology and design, as well as uncompromising service and support.

With support for industry leading communications protocols and technologies, the Multilin 8 Series platform provides easy integration into new or existing SCADA or DCS for enhanced situational awareness.

Vulnerability Details

8 Series family of IEDs supported “Role Based Access Control” since its initial phase. It supports predefined roles Administrator, Operator and Observer. The product manual elaborates on permission

mapped to each role. Overall, the Observer role has read-only access to all device settings. Administrator has read/write access to all device settings. The Operator role has write permission for commands.

GE Vernova received an issue reported by our customer. When we analysed, we could root cause it to role-based permission handling for our output relay configuration -> "Operation" setting. The IED allowed user with "Observer" role to modify this specific output relays setting.

We would like to confirm that this issue is not observed for settings other than mentioned setting.

Also, this issue is not observed in 8 Series IEDs with firmware 4.x onwards.

Affected Products/Versions

Following IEDs of 8 Series family are impacted with this vulnerability.

Products	Versions
8 Series family (850, 845, 889, 869)	All firmware versions till 3.01

Workaround / Mitigation

As a workaround, GE Vernova recommends having sufficient physical access control in place to avoid access to IED by unauthorized personnel.

Resolution

The issue is resolved to make sure user with "observer" role cannot change "output relay operation" setting from HMI. This fix is included in firmware version 3.02.

We strongly recommend Customers using impacted version of 8 Series IEDs to upgrade to the firmware version 3.02. The firmware 3.02 is released for customers already in October 2024.

In case of any query, please reach out to customer support team, GE Vernova.

--- -- ---

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 security@ge.com.

For Product Support

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

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

Document revision history

Version	Date	Change Description
GES-2024-004	4 OCT 2024	Initial release

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.