GE VERNOVA

Grid Solutions

Power Transmission - Digital Products

Security Advisory

Date: **27th January 2026** Distribution: **Public** Reference: **GES-2026-001**

CSD100

V1.5.4

References

Publication number	GES-2026-001
Release date	04th March 2026

Overview

Multiple vulnerabilities are applicable to CSD100 before 1.5.4.
These vulnerabilities were found during development.

Background

CSD100 is an Intelligent Electronic Device, more commonly referred to as a Point-on-Wave controller or Controlled Switching Device. The aim of this controller is to reduce high voltage switching transients that would generate equipment stress, power quality disturbance, and, in worst cases, protection system mis operation, during circuit breaker operation. It is primarily designed to operate independent pole operated circuit breakers (IPO) for both controlled opening and closing operations. CSD100 achieves this by giving open and/or close switching commands to each circuit-breaker pole at the right time, according to a computed sequence.

Exploitation Status

GE Vernova has not yet observed nor received reports of any compromise of Grid Solutions customer equipment due to these vulnerabilities.

Affected Products/Versions

Products	Versions
CSD100	All versions prior to version 1.5.4

1. CVE-2025-24855 on libxslt

a. Vulnerability details

A vulnerability in libxlt could lead to the device to a memory corruption, crash or code execution.

b. CVSS

The vulnerabilities have a score of 7.8.

c. Workaround / Mitigation

GE Vernova recommends that customers implement network protection best practices including firewalls, network segmentation and perimetric protection.

d. Resolution

We strongly recommend Customers to upgrade to the latest version available.

Products	Version
CSD100	1.5.4

2. CVE-2024-40896 in libxml2

a. Vulnerability details

A vulnerability in libxml2 could allow an escalation of privileges with an unauthorized capacity to access or modify resources.

a. CVSS

The vulnerability has a score of 9.1.

b. Workaround / Mitigation

GE Vernova recommends that customers implement network protection best practices including firewalls, network segmentation and perimetric protection.

c. Resolution

We strongly recommend Customers to upgrade to the latest version available.

Products	Version
CSD100	1.5.4

3. CVE-2024-34459 on libxml2

a. Vulnerability details

A vulnerability in libxml2 could result to a buffer over-read and memory access errors.

b. CVSS

The vulnerability has a score of 7.5.

c. Workaround / Mitigation

GE Vernova recommends that customers implement network protection best practices including firewalls, network segmentation and perimetric protection.

d. Resolution

We strongly recommend Customers to upgrade to the latest version available.

Products	Version
CSD100	1.5.4

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@gevernova.com.

For Product Support

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

Region	E-mail
Global Contact GIS	gis_ied_support@gevernova.com
Global Contact AIS	AIS_IED_support@gevernova.com

Document revision history

Version	Date	Change Description
1.0	04th March 2026	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.