GE VERNOVA

Grid Solutions

Power Transmission - Digital Products

Security Notice

Date: **9th December 2025** Distribution: **Public** Reference: **GES-2025-002**

CSD100

V1.5.3

References

Publication number	GES-2025-002
Release date	9th December 2025

Overview

Multiple vulnerabilities are applicable to CSD100 before 1.5.3.
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 1.5.3

1. Denial-of-service 1

a. Vulnerability details

A vulnerability in the TCP management can be used to cause a denial-of-service of TCP-based services CSD100 as web server. However, the opening and closing of circuit breaker are non-impacted by the attack. The TCP-based services are functional one second after the end of attacks.

b. CVSS

The vulnerability has a score of 5.3.

c. Workaround / Mitigation

GE Vernova is actively correcting the vulnerability and will fix the protection in next CSD100 version. GE Vernova recommends to implements good practices of network protection as firewalling, network segmentation and perimetric protection.

d. Resolution

The correction is planned for the next CSD100 version.

2. Denial-of-service 2

a. Vulnerability details

A vulnerability in the SYN TCP management can be used to cause a denial-of-service of the CSD100. In some rare cases, the CSD100 could remain unreachable and needs to be manually rebooted.

b. CVSS

The vulnerability has a score of 7.5

c. Workaround / Mitigation

The vulnerability has been corrected in CSD10 1.5.3 version. GE Vernova recommends to implements good practices of network protection as firewalling, network segmentation and perimetric protection.

d. Resolution

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

Products	Version
CSD100	1.5.3

3. Path traversal vulnerabilities

a. Vulnerability details

Path traversal vulnerabilities allow an authenticated user to access and delete files with an impact on confidentiality and availability.

b. CVSS

The vulnerabilities have a score of 8.8.

c. Workaround / Mitigation

GE Vernova recommends limiting the user numbers and permissions to the needed and creating individual account.

d. Resolution

We strongly recommend Customers to upgrade to the latest version available and **change all passwords**.

Products	Version
CSD100	1.5.3

4. Vulnerabilities on sqlite

a. Vulnerability details

The following CVEs in sqlite could result to a leakage memory or an arbitrary code execution:

- CVE-2025-3277
- CVE-2025-6965

b. CVSS

The vulnerabilities have a score of 9.8.

c. Workaround / Mitigation

GE Vernova recommends to implements good practices of network protection as firewalling, network segmentation and perimetric protection.

d. Resolution

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

Products	Version
CSD100	1.5.3

5. CVE-2024-11235 in PHP

a. Vulnerability details

A vulnerability in PHP could lead to remote execution code.

b. CVSS

The vulnerability has a score of 9.2.

c. Workaround / Mitigation

GE Vernova recommends to implements good practices of network protection as firewalling, network segmentation and perimetric protection.

d. Resolution

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

Products	Version
CSD100	1.5.3

6. Vulnerabilities on zlib

a. Vulnerability details

The CVE could result in a memory corruption or arbitrary code execution:

- CVE-2018-25032

- CVE-2018-25032

b. CVSS

The vulnerability scores have a maximum of 9.8.

c. Workaround / Mitigation

GE Vernova recommends to implements good practices of network protection as firewalling, network segmentation and perimetric protection.

d. Resolution

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

Products	Version
CSD100	1.5.3

7. Multiple CVE in Libexpat

a. Vulnerability details

The following CVEs in Libexpat could allow an attacker to modify memory, allow a deny-of-service or execute non-authorized code:

- CVE-2024-45492
- CVE-2024-45491
- CVE-2024-45490
- CVE-2024-28757
- CVE-2023-52425
- CVE-2022-43680
- CVE-2022-40674
- CVE-2022-25315
- CVE-2022-25314
- CVE-2022-25236
- CVE-2022-25235

b. CVSS

The score of vulnerabilities is a maximum of 9.8.

c. Workaround / Mitigation

GE Vernova recommends to implements good practices of network protection as firewalling, network segmentation and perimetric protection.

d. Resolution

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

Products	Version
CSD100	1.5.3

8. Multiple CVES in in Linux kernel

a. Vulnerability details

Multiple vulnerabilities in Linux Kernel could allow an attacker to modify memory, allow a deny-of-service, escalate privilege or execute remotely non-authorized code:

- CVE-2025-21999
- CVE-2025-21887
- CVE-225-21863
- CVE-2025-21786
- CVE-2025-21786
- CVE-2022-49622
- CVE-2024-50036
- CVE-2024-50067
- CVE-2024-57982
- CVE-2024-56658
- CVE-2024-57951
- CVE-2024-56601
- CVE-2023-5197
- CVE-2024-56606
- CVE-2024-50063

b. CVSS

The score of vulnerabilities is a maximum of 7.8.

c. Workaround / Mitigation

GE Vernova recommends to implements good practices of network protection as firewalling, network segmentation and perimetric protection.

d. Resolution

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

Products	Version
CSD100	1.5.3

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.

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@ge.com
Global Contact AIS	AIS_IED_support@ge.com

Document revision history

Version	Date	Change Description
1.0	9th December 2025	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.