SECURITY ADVISORY

Multiple vulnerabilities on CSD100

CSD100

References

PUBLICATION NUMBER	GES-2026-027
RELEASE DATE	2026-11-10
DISTRIBUTION	Restricted
CVSS	9.2
CVE Identifier	CVE-2026-109618, CVE-2026-109619

Overview

Multiple vulnerabilities are applicable to CSD100 up to (including) 1.5.4.

Please refer to the “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

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 losing 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.

Vulnerability Details

The vulnerability CVE-2026-109618, with a CVSS score of 9.2, allows remote code execution through memory corruption during out-of-memory (OOM) handling. The vulnerability CVE-2026-109619, with a CVSS score of 9.2, allows remote code execution through stale global state.

Affected Products/Versions

PRODUCTS	VERSIONS
CSD100	All firmware versions up to (including) 1.5.4

Workaround / Mitigation

Until the fixed firmware is available, GE Vernova recommends the following to reduce exposure of the CSD100 HTTP web interface:

- Limit all external access to substation networks, and in particular access to CSD100.
- Implement firewall rules to restrict access only from authorized hosts or management subnets.
- Isolate the device in a segmented network zone.
- Monitor network traffic and device logs for suspicious activity.
- Do not expose the web interface to the internet or untrusted networks.

These measures reduce, but do not eliminate, the risk until the fix is installed.

Resolution

GE Vernova is developing a CSD100 firmware update that will address these vulnerabilities. We strongly recommend Customers to apply the mitigations above in the meantime and upgrade as soon as the fixed version is released.

GE Vernova Product Security Incident Response Team (PSIRT)

GE Vernova is committed to helping to ensure the security of its customer base. To report product security issues, contact PSIRT online at https://www.gevernova.com/security.

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

PUBLICATION NUMBER & VERSION	RELEASE DATE	CHANGE DESCRIPTION
GES-2026-027-01	2026-11-10	Initial release

For more information, visit
gevernova.com/electrification

© 2026 GE Vernova and/or its affiliates. All rights reserved. GE and the GE Monogram are trademarks of General Electric Company used under trademark license.

GE VERNOVA