



Security Advisory

Date: 13 March 2026

Distribution: Public

Reference: GES-2026-002

C264 bay controllers

Security Advisory

References

Publication number	GES-2026-002
Release date	13 March 2026
CVSS	9.1 AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:H/A:H (unprotected system) 6.8 AV:N/AC:H/PR:L/UI:N/S:U/C:N/I:H/A:H (secured system)

Overview

The c264 bay controller is a sophisticated modular computer that supports multiple applications and functions for substation control, communications, monitoring, protection and automation. SRP and SRH boards are optional network cards which may be used in C264 bay controllers to provide a PRP or HSR network connection, mainly in DS Agile system v5.x and v6.x. SRP and SRH boards are using Linux kernels which are affected by various critical and high issues.

In DS Agile system v7.x, as C264 bay controllers embed an inbuild network card providing PRP or HSR capabilities, by default, they do not require an SRP or SRH board to be integrated in a PRP or HSR network.

Background

c264 computers and SRP and SRH boards are designed to be installed and operated in a utility and industrial environment and connected to secure private networks.

Vulnerability Details

By having access to SRP board, an attacker could send specifically crafted network frames to the available interfaces to make the SRP board unavailable or rebooting, disconnecting the concerned C264 bay controller from the substation network.

By having access to SRH board, an attacker could send specifically crafted network frames to the available interfaces to make the SRH board unavailable or rebooting, disconnecting the concerned C264 bay controller from the substation network.

Affected Products/Versions

All available SRP and SRH firmware versions are concerned.

Products	Versions
c264 SRPv2 boards	All firmware versions prior to srp282-3.0.0.3 included
c264 SRHv2 boards	All firmware versions prior to srp29x-2.0.0.0 included

Workaround / Mitigation

- Limit all external access to substation networks, and in particular access to the SRP and SRH interfaces via firewall policies.
- Disable Simple Network Management Protocol (SNMP) on SRP and SRH boards, or minimally, use firewall rules to restrict the SNMP connections.
- Be aware that these types of cybersecurity mitigation actions will only work for network traffic that must pass through your firewall.

Resolution

- Replace SRP and SRH boards by switches validated by GE Vernova
- Migrate DS Agile v5.x or v6.x systems using SRP or SRH boards to DS Agile v7.7.x (using on board PRP/HSR capability of CPU4)

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 support team using:

Region	E-mail	Telephone
Global Contact Centre	GA.support@GEVernova.com	+44 1785 250070
Central, East Asia, Pacific	GA.supportCEAP@GEVernova.com	+65 6749 0777
India	GA.supportIND@GEVernova.com	No Phone Line
Middle East, North Africa, Turkey	GA.supportMENAT@GEVernova.com	+971 4 375 6950
Europe, Russia, CIS, Sub-Saharan Africa	ERCIS: GA.supportERCIS@GEVernova.com France: SAM_Aftersales@gevernova.com Poland: support.PLS@gevernova.com Russia: support.AMR@gevernova.com (not in use) UK: support.AGS@gevernova.com	+34 94 4858854
North America	GA.supportNAM@GEVernova.com	+1-877-605-6777 (Global toll-free) +1-800-547-8629 (NAM toll-free) +1-678-844-6777 (Direct)
Latin America	GA.supportLAM@GEVernova.com	+55 48 2108

		0300
--	--	------

Document revision history

Version	Date	Change Description
GES-2026-002	13 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.

