

SECURITY ADVISORY

OS update fixing critical and high security issues

Affected product “H49 switches”

References

PUBLICATION NUMBER	RELEASE DATE	DISTRIBUTION
GES-2025-004	25 September 2025	Public

Overview

Cybersecurity vulnerabilities have been identified in Reason H49 Ethernet Switch, affecting the performance of all product versions. The vulnerabilities are all related to an obsolete and no longer supported version of the Operating System on top of which GE Vernova’s H49 firmware runs. No exploitation of those vulnerabilities on H49 product was brought to GE Vernova’s attention.

Background

Reason H49 is a Redbox switch designed for local area network (LAN) of substation automation systems, providing gigabit redundancy solution for application such as Digital Control System (DCS) and IEC 61850 Digital Substations.

Vulnerability Details

By having access to H49, an attacker could send specifically crafted frames to the available management interfaces to make the H49 unavailable or rebooting.

Affected Products/Versions

All H49 firmware versions prior to 2.1.0 (excluded) are concerned.

PRODUCTS	VERSIONS
H49 Switches	All firmware versions prior to version 2.1.0 excluded

Workaround / Mitigation

- Limit all external access to substation networks, and in particular access to the H49 management interfaces via firewall policies.
- Disable Simple Network Management Protocol (SNMP) on the H49 devices, or minimally, use firewall rules to limit the SNMP.
- Configure the H49 device for centralized access control using the Lightweight Directory Access Protocol (LDAP).
- Be aware that these types of cybersecurity mitigation actions will only work for network traffic that must

pass through your firewall.

- Replace H49 switches by third parties' switches validated by GE Vernova

Resolution

GE Vernova has developed H49-2.1.0 firmware which is running on a recent operating system fixing the vulnerabilities of the firmware prior to 2.1.0.

GE Vernova highly recommends you migrate H49 switches to h49-2.1.0 firmware.

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

Document revision history

PUBLICATION NUMBER & VERSION	RELEASE DATE	DISTRIBUTION
GES-2025-004	25 September 2025	Initial release

For more information, visit
[gevernova.com/electrification](https://www.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.

English
260901