



Security Advisory

Date: **30 May 2024**Distribution: **Public**Reference: **GES-2024-001**

H49 switches Security Advisory

References

Publication number	GES-2024-001
Release date	30 May 2024

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 obsoleted and no longer supported version of the Operating System that our H49 firmware runs on top of.

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 sent specifically crafted frames to the available management interfaces to make the H49 unavailable or rebooting.

Affected Products/Versions

All H49 firmware versions prior to 2.0.3.1 (included) are concerned.

Products	Versions
H49 switches	All firmware versions prior to version 2.0.3.1 included

Workaround / Mitigation

- Limit all external access to substation networks, and in particular access to the H49 management interfaces via firewall policies.
- Disable SNMP on the H49 devices, or minimally, use firewall rules to limit the SNMP.
- Configure the H49 device for centralized access control using the LDAP protocol.
- 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 is committed to helping ensure the security of its customer base, and a new firmware version will be made available to upgrade the operating system and to address the present vulnerabilities.

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 PSIRT@gevernova.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	+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

Version	Date	Change Description
GES-2024-001	30 May 2024	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.