



Security Notice

Date: **04 June 2025**Distribution: **Public**Reference: **GES-2025-003**

MCP (G500, G100)

References

Publication number	GES-2025-003
Release date	04 June 2025

Overview

The Multi-function Controller Platform (i.e., G500, G100) has a few vulnerabilities that are fixed in v5.2. These vulnerabilities were found during development and/or by customers.

Background

GE Vernova's Multi-function Controller Platform (MCP) is a platform that offers a high-capacity, secure, substation-hardened set of modular and expandable hardware and software components designed to simplify deployment, operation, and maintenance of automation systems. MCP is designed to provide a reliable and accurate collection of data (metering, status, events, and faults) from serial or LAN based intelligent substation devices to master applications such as SCADA, EMS, DMS or other enterprise applications.

Vulnerability Details

The following issues were fixed:

Issue	Severity
Privilege Escalation Direct Access to Page Allowed: Some files are exposed on the HMI web without proper authentication. In particular, configured oneline drawing file(s), which can contain sensitive information about the system.	High, if oneline is configured.
Command Injection in Time Zone Search. This is specific to time zone configuration in the MCP Web Settings. <i>Fixed in MCP (G500, G100) v4.0.</i>	Medium
Ability to Mount PETC Filesystems. More specifically, the ability for an administrator user to view and modify contents/mount Host disks.	Medium
Container Escape via Sys_Module Capabilities.	Assessed as medium in MCP deployment since an administrator must be logged in for the vulnerability to be exploited.
Control Group Container Escape (CVE-2022-0492).	High as marked by the CVE, but assessed as medium in MCP deployment since an administrator must be logged in for the vulnerability to be exploited.
Missing input validation on Local HMI Login prompt.	Medium
SSH Terrapin Prefix Truncation Weakness (CVE-2023-48795). The remote SSH server is vulnerable to a man-in-the-middle prefix truncation attack.	Medium

Affected Products/Versions

Products	Versions
MCP (G500, G100)	All firmware versions prior to version 5.2, except where explicitly mentioned otherwise in the Vulnerability Details.

Workaround / Mitigation

MCP (G500, G100) v5.2 include fixes to the vulnerabilities described above.

Resolution

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

Products	Versions
G500	V5.2
G100	V5.2

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@ge.com.

Contact Technical Support

GE Vernova Grid Solutions Technical Support is open 24 hours a day, seven days a week for you to talk directly to a GE Vernova representative.

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-2025-003	04 June 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.