SECURITY ADVISORY

Buffer overflow vulnerability

Affected product: Multi-function Controller Platform (MCP) with firmware version v5.4 or earlier

References

PUBLICATION NUMBER	GES-2026-015
RELEASE DATE	2026-11-05
DISTRIBUTION	Restricted
CVSS	9.2
Environmental Score	6.7 after mitigation. New CVSS v3.1 Vector AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/CR:X/IR:X/AR:X/MAV:L/MAC:X/MPR:H/MUI:X/MS:X/MC:X/MI:X/MA:X
CVE Identifier	CVE-2026-111497

Overview

A critical buffer overflow and out-of-bounds write vulnerability in the Google Brotli compression library permits unauthenticated remote code execution (RCE).

This flaw impacts the remote MCP Settings GUI as the interface bundles the vulnerable Brotli decoder to power web-based Graphical User Interfaces for configuring and managing the Mutli-function Controller Platform (MCP) device including G500 and G100.

This vulnerability is not applicable to any port/communication configured as an external zone.

Please refer to the “Vulnerability details” section for impacted version & weakness details.

At the time of publication of this document, there were no reported cybersecurity attacks which exploited this vulnerability. GE Vernova is addressing this vulnerability as part of its commitment to improve security in our products.

Background

CVE-2026-111497 (also known as Node2Shell, HTTP2Shell, or Broccoli2Shell) is a critical buffer overflow and out-of-bounds write vulnerability in the Google Brotli compression library.

An unauthenticated remote attacker can send a crafted, malformed Brotli-compressed data stream to an exposed application, triggering a write past the end of a memory buffer and potentially executing arbitrary code with the application's privileges.

Vulnerability Details

This vulnerability affects any software or runtime that bundles or dynamically uses vulnerable versions of the Google Brotli decoder (versions 1.0.3 through 1.2.0).

This vulnerability affects part of the code used in the remote MCP Settings GUI to act as the embedded web server & API backend. The remote MCP Settings GUI is a "web-based equivalent" of the local mcpcfg command-line utility, accessed via a standard web browser (Internet Explorer, Microsoft Edge, Mozilla Firefox, Google Chrome) over HTTPS on port 8081.

Due to this vulnerability, the capabilities governed through the remote MCP Settings GUI would be exposed, such as:

- Authentication control - Configure Authentication, switch between Local/Remote authentication modes, create/modify Admin users.
- Network/Firewall reconfiguration - Configure Network Settings, Network Interfaces, and Firewall rules, potentially exposing internal ports to external scanners if the firewall is altered or disabled.
- System resets/destructive actions - Reset System Logs, Reset Database Tables, Reset File Persistence Data, Restore to Factory Default, and Reboot Device.

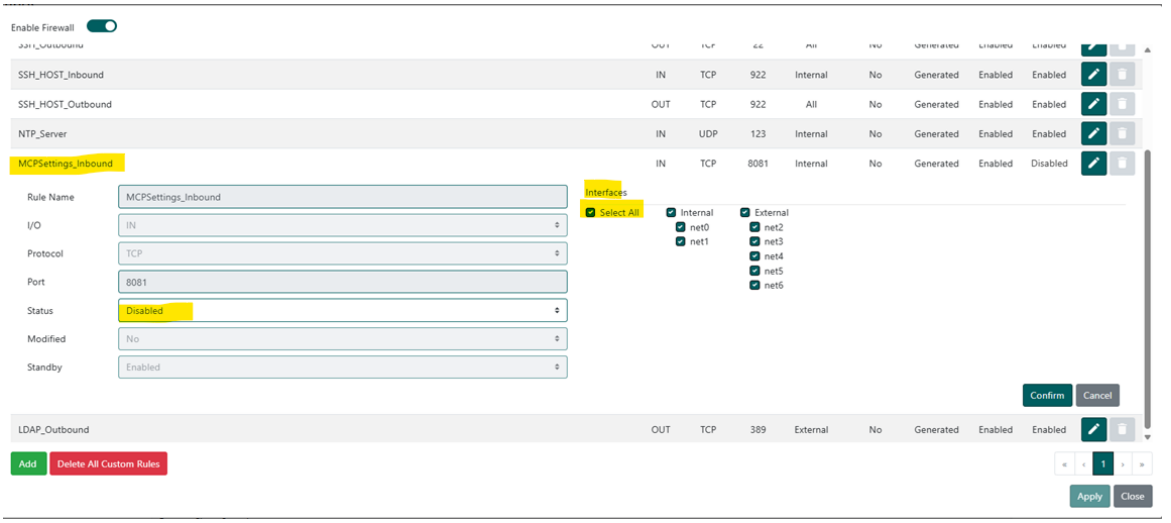
Affected Products/Versions

PRODUCTS	VERSIONS
MCP devices including G500 and G100	All firmware versions up to version MCPv5.4

Workaround / Mitigation

The mitigation for MCPv5.4 or earlier versions:

- Using the local MCP Settings GUI or the "mcpcfg" command line utility to block the MCP Settings GUI TCP port 8081 (remote MCP Settings GUI) on all interfaces by disabling the "*MCPSettings_Inbound*" rule as follows:



- With the mitigation in place, the user can still configure the MCP settings using "mcpcfg" command line utility or local MCP Settings GUI through local MCP connection (KVM connection).

Resolution

This issue will be fixed in MCPv5.5 and v6.0.

We strongly recommend Customers to upgrade to the MCPv5.5 or later once it is available.

GE Vernova Product Security Incident Response Team (PSIRT)

To report product security issues and to request security support, contact PSIRT online at https://www.gevernova.com/security.

For more information, visit
gevernova.com/electrification

GE VERNOVA

© 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

For Product Support

For questions or further product support, please contact the GE Vernova support team using

REGION	E-MAIL	TELEPHONE
Global Contact Center	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 France: SAM_Aftersales@gevernova.com Poland: support.PLS@gevernova.com UK: support.AGS@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	CHANGE DESCRIPTION
GES-2026-015-01	2026-11-05	Initial release

For more information, visit
gevernova.com/electrification

GE VERNOVA

© 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