

Password Authentication Bypass Vulnerability in GX Works3 and Motion Control Setting

Release date: September 17, 2026
Mitsubishi Electric Corporation

Overview

A password authentication bypass vulnerability due to Incorrect Implementation of Authentication Algorithm (CWE-303¹) exists in the Block Password function for GX Works3 and Motion Control Setting. A local attacker may be able to successfully authenticate even with an invalid block password by executing the affected product and modifying part of the executable module in memory, and thereby may be able to view, tamper with, destroy, or delete control programs (CVE-2026-15688).

The product names and versions affected by this vulnerability are listed below.

CVSS²

CVE-2026-15688 CVSS:4.0/AV:L/AC:L/AT:N/PR:L/UI:N/VC:H/VI:H/VA:N/SC:N/SI:H/SA:H Base Score:9.2

Affected products

<Products and Versions>

Product Name	Versions
GX Works3	All versions
Motion Control Setting (*1)	All versions

(*1) Software packaged with GX Works3

<How to Check the Versions>

- GX Works3 : Please refer to "Checking the version of GX Works3" in "1.9 Learning Operation Methods of GX Works3" of the "GX Works3 Operating Manual". The manual can be viewed using the "e-Manual Viewer" included with GX Works3.
- Motion Control Setting : Please refer to "Checking the version of Motion Control Setting Function" in "1.2 Learning Operation Methods of Motion Control Setting Function" of the "Motion Control Setting Function Help".

Description

A password authentication bypass vulnerability (CVE-2026-15688) due to Incorrect Implementation of Authentication Algorithm (CWE-303) exists in the Block Password function for GX Works3 and Motion Control Setting.

Impact

A local attacker may be able to successfully authenticate even with an invalid block password by executing the affected product and modifying part of the executable module in memory, and thereby may be able to view, tamper with, destroy, or delete control programs.

Countermeasures for Customers

Please apply the mitigations and workarounds described in the " Mitigations / Workarounds" section.

Mitigations / Workarounds

The table below shows workarounds for each product.

No.	Product Name	Workarounds
1	GX Works3	Download Ver. 1.096A or later, update the software, and set security version for project to "2". Please refer to "15.9 Preventing Illegal Access to/Falsification of Data (Security Version)" in "GX Works3 Operating Manual" for details.
2	Motion Control Setting	Download Ver. 1.070Y or later, update the software, and set security version for project to "2". Please refer to "12.5 Preventing Illegal Access to/Falsification of Data (Security Version)" in "Motion Control Setting Function Help" for details. In addition, please apply the workaround for GX Works3 described in No. 1 of this table.

¹ <https://cwe.mitre.org/data/definitions/303.html>

² <https://www.first.org/cvss/v3.1/specification-document>

The table below lists the download locations for update software and the installation procedures for each product.

No.	Product Name	Download location	Installation Procedure
1	GX Works3	https://www.mitsubishielectric.com/fa/download/software/detailsearch.page?mode=software&kisyu=/plceng&shiryoide=1000001411&lang=2&select=0&softid=1&infostatus=1_2_1&viewradio=0&viewstatus=&viewpos=	1. Unzip the downloaded file (zip format). 2. Execute the installer in the unzipped folder to install.
2	Motion Control Setting	https://www.mitsubishielectric.com/fa/download/software/detailsearch.page?mode=software&kisyu=/ssc&shiryoide=100000803&lang=2&select=0&softid=1&infostatus=1_8_1&viewradio=0&viewstatus=&viewpos=	

Mitsubishi Electric recommends that customers take the following mitigation measures to minimize the risk of this vulnerability being exploited:

- Use your computer with the affected product within the LAN and block remote login from untrusted networks, hosts, and users.
- Use a firewall, virtual private network (VPN), etc., to prevent unauthorized access, and allow remote login only for trusted users when connecting your computer with the affected product to the Internet.
- Do not click web links contained in emails or other messages from untrusted sources. Also, do not open attachments in untrusted emails.
- Install antivirus software on your computer running the affected product.
- Restrict physical access to your computer on which the affected product is installed, as well as to computers and network devices that can communicate with it.

Acknowledgement

Mitsubishi Electric would like to thank Mayeul Fargier, Erwan Cordier, and Noé Flatreaud who reported this vulnerability.

Contact information

Please contact your local Mitsubishi Electric representative.

<Inquiries | MITSUBISHI ELECTRIC FA>

<https://www.mitsubishielectric.com/fa/service-support/index.html>