Information Disclosure Vulnerability in GX Works2

Release date: November 27, 2025
Mitsubishi Electric Corporation

Overview

An information disclosure vulnerability exists in GX Works2. GX Works2 stores credential information in plaintext, allowing an attacker to disclose these plaintext credential information from project files. As a result, the attacker may be able to open project files protected by user authentication using disclosed credential information, and obtain or modify project information. (CVE-2025-3784)

CVSS[1]

CVE-2025-3784 CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N Base score 5.5

Affected products

All versions of GX Works2 are affected.

Description

An information disclosure vulnerability due to Cleartext Storage of Sensitive Information (CWE-312[2]) exists in GX Works2.

Impact

An attacker could disclose credential information stored in plaintext from project files. As a result, the attacker may be able to open project files protected by user authentication using disclosed credential information, and obtain or modify project information.

Countermeasures for Customers

The fixed version for this vulnerability is currently under development.
Until the fixed version is released, please take the mitigations described below.

Mitigations / Workarounds

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

- Use the PCs with the affected product installed in the LAN and block remote logins from untrusted networks, hosts, or users.
- Block unauthorized access by using a firewall or a virtual private network (VPN), etc., and allow remote logins only for trusted users when connecting the PCs with the affected product installed to the internet.
- Restrict physical access to the PCs with the affected product installed, as well as to PCs and network devices that can communicate with those PCs.
- Install an antivirus software on the PCs running the affected product.
- Encrypt project files when sending or receiving them over the internet.

Acknowledgement

Mitsubishi Electric would like to thank Jiho Shin(M.S. graduate, Sungkyunkwan University) who reported this vulnerability.

Contact information

Please contact your local Mitsubishi Electric representative.

<Contact address: Mitsubishi Electric FA>
https://www.mitsubishielectric.com/fa/support/index.html

[1] https://www.first.org/cvss/v3.1/specification-document

[2] https://cwe.mitre.org/data/definitions/312.html