Information Disclosure Vulnerability in GT Designer3

Release date: December 16, 2025
Mitsubishi Electric Corporation

Overview

Information Disclosure vulnerability due to Cleartext Storage of Sensitive Information(CWE-312[1]) exists in GT Designer3. GT Designer3 stores credentials and verifies them in plain text, therefore an attacker may be able to obtain plaintext credentials from the project file for GT Designer3. As a result, the attacker may be able to operate illegally GOT2000 series or GOT1000 series by using the obtained credentials (CVE-2025-11009).

CVSS [2]

CVE-2025-11009 CVSS:3.1/AV:L/AC:H/PR:N/UI:N/S:U/C:H/I:N/A:N Base Score:5.1

Affected products

The following products are affected:
< Products and Versions >
- GT Designer3 Version1 (GOT2000), all versions
- GT Designer3 Version1 (GOT1000), all versions

Description

Information Disclosure vulnerability due to Cleartext Storage of Sensitive Information(CWE-312) exists in GT Designer3.

Impact

An attacker may be able to obtain plaintext credentials from the project file for GT Designer3. As a result, the attacker may be able to operate illegally GOT2000 series or GOT1000 series by using the obtained credentials.

Countermeasures

There are no plans to release a fixed version addressing this vulnerability. Please carry out mitigations/workarounds.

Mitigations / Workarounds

Mitsubishi Electric recommends that customers take the following mitigation measures to minimize the risk of exploiting this vulnerability:
- Use your personal computer with the affected product within the LAN and block remote login from untrusted networks, hosts, and users.
- When connecting your personal computer with the affected product to the Internet, use a firewall, virtual private network (VPN), etc., to prevent unauthorized access, and allow only trusted users to remote login.
- Install an antivirus software in your personal computer using the affected product.
- Don’t open untrusted files or click untrusted links.

Acknowledgement

Mitsubishi Electric would like to thank Hea-Eun Moon and Junbeom Gwak from the Red Alert Lab at NSHC who reported this vulnerability.

Contact information

Please contact your local Mitsubishi Electric representative.
<Inquiries | MITSUBISHI ELECTRIC FA>
https://www.mitsubishielectric.com/fa/support/index.html

[1] https://cwe.mitre.org/data/definitions/312.html
[2] https://www.first.org/cvss/v3.1/specification-document