

# Password authentication bypass vulnerability in VNC function of GOT

Release date: April 22, 2021  
Mitsubishi Electric Corporation

## ■ Overview

A password authentication bypass vulnerability exists in VNC function of GOT2000 series and GOT SIMPLE series due to improper authentication. When the VNC server configuration is enabled, a malicious attacker can gain unauthorized access by sending specially crafted packets. (CVE-2021-20590)

## ■ CVSS Score

CVE-2021-20590 CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:H/A:N Base Score:5.9

## ■ Affected products

Affected products and versions are below.

Affected when using the "VNC server" function.

| Series            | Model      | Product Name  | VNC server version |
|-------------------|------------|---------------|--------------------|
| GOT2000 series    | GT27 model | All           | All versions       |
|                   | GT25 model | All           | All versions       |
|                   | GT21 model | GT2107-WTBD   | All versions       |
|                   |            | GT2107-WTSD   |                    |
| GOT SIMPLE series | GS21 model | GS2110-WTBD-N | All versions       |
|                   |            | GS2107-WTBD-N |                    |

## ■ Description

A password authentication bypass vulnerability exists in VNC function of GOT2000 series and GOT SIMPLE series due to improper authentication (CWE-287).

## ■ Impact

When the VNC server configuration is enabled, a malicious attacker can gain unauthorized access by sending specially crafted packets.

## ■ Countermeasures

Please carry out the mitigations below. We will release a fixed version in the near future.

## ■ Mitigations

Please restrict access to the product only from trusted networks and hosts.

## ■ Contact information

Please contact your local Mitsubishi Electric representative.

< Inquiries | MITSUBISHI ELECTRIC FA >

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