Password authentication bypass vulnerability in VNC function of GOT

■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"funcition.

Series	Model	Product Name	VNC server version
GOT2000 series	GT27 model	All	01.39.010 and prior
	GT25 model	All	01.39.010 and prior
	GT21 model	GT2107-WTBD	01.40.000 and prior
		GT2107-WTSD	
GOT SIMPLE series	GS21 model	GS2110-WTBD-N	01.40.000 and prior
		GS2107-WTBD-N	

〈How to check the versions in use〉

For how to check the versions in use, please refer to the following manual. The latest version of manual is available from MITSUBISHI ELECTRIC FA Global Website (https://www.mitsubishielectric.com/fa).

For GT27/GT25 models
GOT2000 Series User's Manual (Utility) (SH-081195ENG)
"6.9 Package Data Management" - "Property operation"

For GT21/GS21 models
GOT2000 Series User's Manual (Utility) (SH-081195ENG)
"15.2 OS information"

■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

In the case of using the affected products and versions, please update to the fixed versions by following the steps below.

<Fixed versions>

The fixed versions for the vulnerability is below.
(Fixed "VNC server"function is included in GT Designer3 Version1 (GOT2000) Ver.1.260W or later.)

Series	Model	Product Name	Fixed VNC server versions
GOT2000 series	GT27 model	All	01.40.000 or later
	GT25 model	All	01.40.000 or later
	GT21 model	GT2107-WTBD	01.41.000 or later
		GT2107-WTSD	
GOT SIMPLE series	GS21 model	GS2110-WTBD-N	01.41.000 or later
		GS2107-WTBD-N	

<Update procedure>

1) Download the fixed version of GT Designer3 Version1 (GOT2000) and install it on your personal computer.
Please contact your local Mitsubishi Electric representative about GT Designer3 Version1 (GOT2000).
2) Start the GT Designer3 Version1 (GOT2000) and open the project data used in affected products.
3) Select [Write to GOT] from [Communication] menu to write the required package data to the GOT.
＊Please refer to "4. COMMUNICATING WITH GOT" in the GT Designer3 (GOT2000) Screen Design Manual (SH-081220ENG).
4) After writing the required package data to the GOT, refer to the <How to check the versions in use> and check that the driver has been updated to the fixed versions.

■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

■Trademarks

VNC is a registered trademark of RealVNC Ltd. in United States and other countries.

■Update history

July 27, 2021

Added "How to check the versions in use" to "Affected products".
Added "Update procedure" and "Fixed Versions" to "Countermeasures".