Release date: Mar 17th, 2023

CONTEC CO., Ltd

Vulnerability in CONPROSYS IoT Gateway

■ Overview

Contec has identified several vulnerabilities in its CONPROSYS M2M Gateway and CONPROSYS M2M Controller IoT gateway products (hereinafter referred to as “CONPROSYS IoT gateway products”). These vulnerabilities could be exploited by a malicious attacker to steal or tamper with data or to execute malicious programs that could result in the destruction of the system.

The products affected by these vulnerabilities and the countermeasures/workarounds are listed below. Please implement the appropriate countermeasures or workarounds as soon as possible.

■ Affected products

Model: CONPROSYS M2M Gateway Series, M2M Controller Series

Type:

1. M2M Gateway (5 models)
   CPS-MG341-ADSC1-111, CPS-MG341-ADSC1-931, CPS-MG341G-ADSC1-111, CPS-MG341G-ADSC1-930, CPS-MG341G5-ADSC1-931
2. M2M Controller Integrated Type (9 models)
   CPS-MC341-ADSC1-111, CPS-MC341-ADSC1-931, CPS-MC341-ADSC2-111, CPS-MC341G-ADSC1-110, CPS-MC341Q-ADSC1-111, CPS-MC341-DS1-111, CPS-MC341-DS11-111, CPS-MC341-DS2-911, CPS-MC341-A1-111
3. M2M Controller Configurable Type (5 models)
   CPS-MCS341-DS1-111, CPS-MCS341-DS1-131, CPS-MCS341G-DS1-130, CPS-MCS341G5-DS1-130, CPS-MCS341Q-DS1-131

   Version: 1. Ver.3.7.10 and earlier
   2. Ver.3.7.6 and earlier
   3. Ver.3.8.8 and earlier

■ The vulnerability and its threat

[JVNVU#96198617]

1. CVE-2023-27917: ” OS command injection in CONPROSYS IoT gateway products ”
   This vulnerability makes it possible for OS execution commands to be input from Network Maintenance page. These commands could then be used by a malicious attacker to steal or tamper with information, destroy the system, or execute malicious programs when logged into the management screen.
   CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H Basic Score : 8.8
2. CVE-2023-27389: ” Insufficient encryption in CONPROSYS IoT gateway products ”
   Due to insufficient encryption, this vulnerability makes it possible for a malicious attacker to analyze and replace files used to update the product software with malicious firmware that allows the attacker to tamper with or destroy the system or to execute malicious programs.
   CVSS:3.1/AV:N/AC:H/PR:H/UI:N/S:U/C:H/I:H/A:H Basic Score : 6.6
3. CVE-2023-23575: ” Inadequate access restrictions in CONPROSYS IoT gateway products ”
   This vulnerability makes it possible for users with normal privileges to access Network Maintenance page, which should only be accessible by administrators. This makes it possible for a malicious attacker to steal network information or other information.
   CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:L/I:N/A:N Basic Score : 4.3

■ Fix Version

By installing the latest version on CONTEC's website, the above vulnerabilities can be fixed.

1. M2M Gateway

https://www.contec.com/download/donwload-list/?itemid=f832c526-dcf6-4976-85aa-f536c15a8120#firmware

2. M2M Controller Integrated Type

https://www.contec.com/download/donwload-list/?itemid=a054b3eb-da97-40d0-9598-d7f5ff4239ec#firmware

3. M2M Controller Configurable Type
https://www.contec.com/download/donwload-list/?itemid=a1b33f0d-d32b-4549-9741-613cd37d5528#firmware

■ Workarounds

For customers unable to update to the latest version, Contec recommends the following workarounds to minimize the risk of exploitation of these vulnerabilities by an attacker.

- Set up a firewall at an upstream location in the network where the product is being used.
- Limit network access for this product to a reliable closed network.
- Change the product's user and password settings from the default settings.
- Regularly change the product's user and password settings.

■ Related information

- JVNVU#96198617 "Multiple vulnerabilities in Contec CONPROSYS IoT gateway products"
  https://jvn.jp/en/vu/JVNVU96198617/

■ Contact Information

Technical Support Center
https://www.contec.com/support/technical-support/