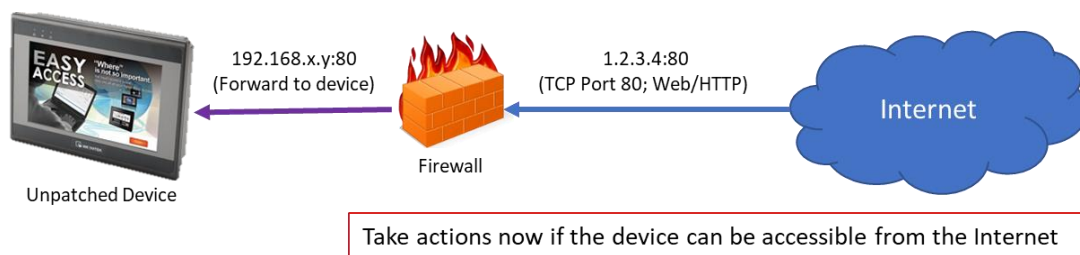# Technical Notice

2021-03-17 (Rev. 1)

Summary

According to ICSA-20-077-01, security issues are found in EasyWeb V1.1 on cMT devices.

If these devices are exposed to an open network, like below, we strongly suggest customers to disconnect the device from the network and upgrade the operating system (OS).

If these devices are not connected to an open network, they may not be affected but we still suggest customers to upgrade the OS.

A device is said to be exposed to an open network, if it can be accessed by a public IP (meaning an IP address NOT like 192.168.x.y, 172.16.x.y with 16 varied from 16 to 31, or 10.x.y.z). For example, you can directly access the device from your home with the firewall's IP address. In the example below, it can be access by typing http://1.2.3.4:80 in the web browser. Note that the firewall must have been configured to allow this operation.

192.168.x.y:80
(Forward to device)

1.2.3.4:80
(TCP Port 80; Web/HTTP)

Internet

Firewall

Unpatched Device

Take actions now if the device can be accessible from the Internet

A device accessible to the Internet (firewall is configured to forward the packet)

Description

According to ICSA-20-077-01, security issues are addressed with EasyWeb V1.1 running on cMT devices. EasyWeb provides the configuration web interface for cMT devices.

A remote attacker may gain access to the system or remotely execute commands without authentication via the web server whose version is below V1.2 (not included).

If the device mentioned above is connected an open network, meaning the device can be accessed by anyone, we strongly suggest customers to:

(1) Disconnect the device from the open network

(2) Upgrade the OS of the device

(3) (Optional) Use EasyAccess 2.0 (our secured VPN service) to access the device so there is no need to expose the device directly to the Internet. EasyAccess 2.0 is a VPN-based remote access solution providing secure connections between PC/Android/iOS and the devices.
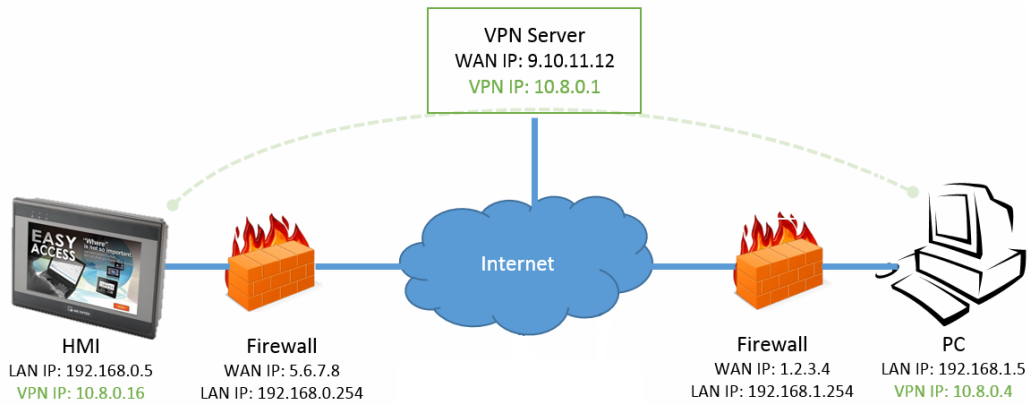
EasyAccess 2.0 Network Overview

Some examples of an open network:

a) Device is connected to a router which is configured to forward TCP port 80 to the device. In this case, you can access the device via a public IP not in the same network.

b) The device is connected to a network where guests or anyone have access to such as an open Wi-Fi network.

Affected Range

The security issues are found in the unpatched web service, EasyWeb V1.1, which is already running on the cMT products listed below.

A device is affected only if the following two conditions are met:

(1) It is connected to an open network where a remote attacker may have access to.

(2) It is using the following OS version:

#	Model	Affected OS Version
1	cMT-SVR-1xx/2xx	< 20210305 (not included)
2	cMT-G01/G02	< 20210209 (not included)
3	cMT-G03/G04	< 20210222 (not included)
4	cMT3071/cMT3072/cMT3090/cMT3103/cMT3151	< 20210218 (not included)
5	cMT-HDM	< 20210204 (not included)
6	cMT-FHD	< 20210208 (not included)
7	cMT-CTRL01	< 20210302 (not included)

Find Current OS Version

For model no. 1, 2 and 3 (models without screen), OS version is available in the web page as shown below.

For model no. 4, 5, 6, and 7 (models with screen), OS version is available via web page and on-screen system setting page:
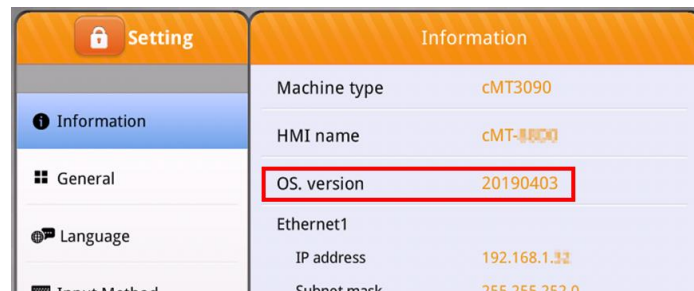
Solution

We have prepared OS upgrade images for the affected products. After downloading the corresponding images, please follow the OS upgrade guide carefully. Do not power cycle the device during the update as the update will be broken and the device may be broken.

#	Model	OS image	OS upgrade guide
1	cMT-SVR-1xx/2xx	cMT_SVR_OS_20210305.zip (contact our distributors for the file)	PDF See 1.10 How to update cMT-SVR OS image
2	cMT-G01/G02	cMT_G01_G02_OS_20210209.zip (contact our distributors for the file)	PDF See 3.2 Updating OS
3	cMT-G03/G04	cMT_G03_G04_OS_20210222.zip	PDF (cMT-G03)

		(contact our distributors for the file)	PDF (cMT-G04) See 3.2 Updating OS
4	cMT3071/cMT3072/ cMT3090/cMT3103/ cMT3151	cMT3071_3072_3090_3151_OS_20210218.zip (contact our distributors for the file)	PDF
5	cMT-HDM	cMT_HDM_OS_20210204.zip (contact our distributors for the file)	PDF
6	cMT-FHD	cMT_FHD_OS_20210208.zip (contact our distributors for the file)	PDF
7	cMT-CTRL01	cMT_CTRL_OS_20210302.zip (contact our distributors for the file)	PDF See 3.2 Updating OS