# Vulnerability in SVM Series

15/9/2022

## Summary

There is a vulnerability in SVM series that allows a login password to be obtained from SVM controller via LAN.

## Affected systems

SVMPC1 Ver2.1.22 or earlier version

SVMPC2 Ver1.2.3 or earlier version

## Detailed information

Files in a specific directory in the SVM controller can be read by accessing the SVM controller with a Web browser from a PC, smartphone or other device in the LAN to which the SVM controller is connected. In this specific directory, there is a file that contains the login password to SVM. An attacker can login to the SVM as a authenticated user by obtaining this information.

## Possible impact

An attacker can login to SVM as an authorized user by obtaining the login password. Then the attacker operates air-conditioner and other equipment connected to the SVM. It is also possible to change automatic control settings like schedule function of the SVM.

Note: Access privileges to the LAN to which the SVM controller is connected is required to obtain the login password using this vulnerability. In addition, attacker cannot get login password from the Internet even if using this vulnerability, if the SVM controller has been installed with SVM standard installation configuration.

## Countermeasures

Update program that resolves this vulnerability is automatically installed if internet access setting of the SVM controller has enabled. No user operation is required.

In case SVM controller has disabled internet access setting, once internet access setting change to enable and connect the SVM controller to a LAN that SVM controller can access to the Internet, then the SVM controller will be updated automatically during the night.

DAIKIN Holdings Singapore PTE LTD

https://www.daikin-solutions.com