Vulnerability Disclosure – Altivar Process ATV600

9/30/2015

Overview

Schneider Electric has become aware of several vulnerabilities in the Ethernet module of its Altivar Process ATV600 products.

The vulnerabilities identified include:

1. FTP service accessible to end users allowing a user to modify software scripts, and configuration information including web server credentials.
2. Hardcoded credentials on the FTP server that enable access to the previous information.
   Default credentials on the HTTP server that enables illegal access to the product.

Vulnerability Overview

Please note that all of these vulnerabilities require network access to the target device. These vulnerabilities were discovered by Schneider Electric internal investigations. Schneider Electric has no evidence that these vulnerabilities have been exploited at customer sites.

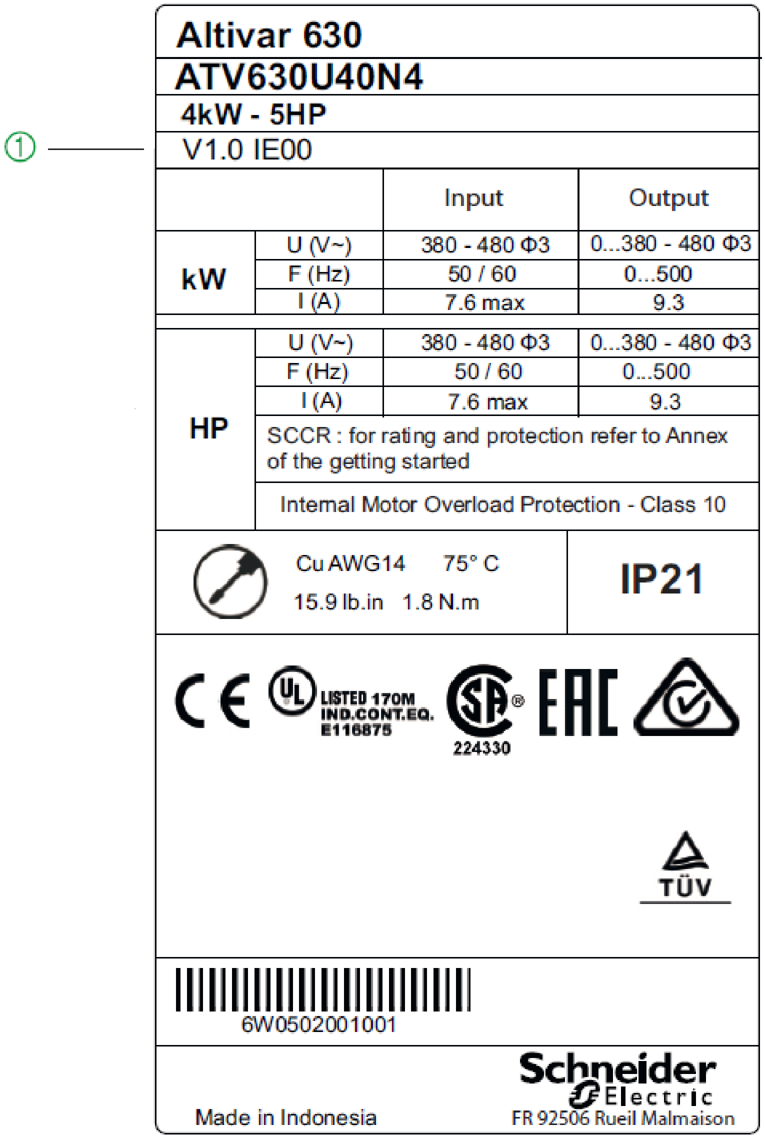
Default credentials of the FTP server may lead to illegal access to the FTP server of the Ethernet communication module. Major information like software scripts or security information may be accessed in read and write modes.
Default credentials of the HTTP server if unchanged may lead to illegal access to the Web server.

Overall CVSS score = 8.3
(AV:N/AC:L/Au:S/C:P/I:P/A:C/E:H/RL:U/RC:C/CDP:MH/TD:H/CR:H/IR:M/AR:L)

Product(s) Affected

- ATV630/650 version V1.1
- ATV630/650 version V1.2
- ATV630/650 version V1.3

The product version can be easily identified using the nameplate on your product.



Altivar 630

ATV630U40N4

4kW - 5HP

① V1.0 IE00

		Input	Output
kW	U (V~)	380 - 480 Φ3	0...380 - 480 Φ3
	F (Hz)	50 / 60	0...500
	I (A)	7.6 max	9.3
HP	U (V~)	380 - 480 Φ3	0...380 - 480 Φ3
	F (Hz)	50 / 60	0...500
	I (A)	7.6 max	9.3

SCCR : for rating and protection refer to Annex of the getting started

Intemal Motor Overload Protection - Class 10

Cu AWG14 75° C

15.9 lb.in 1.8 N.m

IP21

LISTED 170M IND.CONT.EQ. E116875

224330

TÜV

6W0502001001

Made in Indonesia

Schneider Electric
FR 92506 Rueil Malmaison

Mitigation

To help to secure the access to the Power Drive System, the following mitigation must be applied:

- Do not expose your Power Drive System to open networks when not needed
- If your Power Drive System is accessed on an open network, make sure that a firewall is used and that the FTP service is filtered
- If you do not use the HTTP server, disable this feature.
- If the HTTP server is used, make sure to change the default password to reduce the risk of unauthorized access.

For more information, refer to the
Altivar Process ATV600 programming manual: (EAV64318)
to disable the Webserver server.

http://www.schneider-electric.com/ww/en/download/document/EAV64318

For More Information

This document is intended to help provide an overview of the identified vulnerability and actions required to mitigate it. To obtain full details on the issues and assistance on how to protect your installation, please contact your local Schneider Electric representative. These organizations will be fully aware of the situation and can support you through the process.

For further information on vulnerabilities in Schneider Electric’s products, please visit Schneider Electric’s cybersecurity web page at

http://www2.schneider-electric.com/sites/corporate/en/support/cybersecurity/cybersecurity.page

About Schneider Electric

As a global specialist in energy management with operations in more than 100 countries, Schneider Electric offers integrated solutions across multiple market segments, including leadership positions in Utilities & Infrastructures, Industries & Machine Manufacturers, Non-residential Buildings, Data Centers & Networks and in Residential.
www.schneider-electric.com