

Important Security Notification

Security Notification – SoMove

1-Mar-2018

Overview

Schneider Electric has become aware of a vulnerability identified in SoMove software and DTM software components.

Vulnerability Overview

The vulnerability identified is

- DLL Hijacking

SoMove application is a commissioning tool to configure variable speed drives. The application requires the installation of software components called DTM software to support the different types of Variable Speed Drives.

The vulnerability allows an attacker to execute arbitrary code in Schneider Electric SoMove software and associated DTM software components. By hijacking some DLLs, an attacker can force the process to load arbitrary DLL and execute arbitrary code in the context of the process.

Product(s) Affected

The affected Schneider Electric software are listed in the following table:

Software components	Software Package	Vulnerable versions
SoMove Software	SoMove	Version < V2.6.2
ATV320 DTM	Schneider_Electric_Altivar_Machine_ATV320_DTM_Library	Version < V1.1.6
ATV340 DTM	Schneider_Electric_Altivar_Machine_ATV340_DTM_Library	Version < V1.2.3
ATV6xx DTM	Schneider_Electric_Altivar_Process_ATV6xx_DTM_Library	Version < V1.8.0
ATV9xx DTM	Schneider-Electric-Altivar-Process-ATV9xx-DTM-Library	Version < V1.3.5
ATV32 DTM	AltivarDtmLibrary	Version < V12.7.0
ATV71 DTM	AltivarDtmLibrary	Version < V12.7.0
ATV61 DTM	AltivarDtmLibrary	Version < V12.7.0
ATV LIFT DTM	AltivarDtmLibrary	Version < V12.7.0
ATV31/312 DTM	AltivarDtmLibrary	Version < V12.7.0
ATV212 DTM	AltivarDtmLibrary	Version < V12.7.0
ATV12 DTM	AltivarDtmLibrary	Version < V12.7.0

Important Security Notification

Vulnerability Details

The following CVSS score has been assessed for the identified vulnerability:

Overall CVSS Score: 7.8 (High)

(CVSS V3 Vector): CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

CVE ID: CVE-2018-7239 <https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-7239>

Mitigation

Updates for the affected software packages are included for download below:

- SoMove Software - SoMove_V2.6.3
https://www.schneider-electric.com/en/download/document/SoMove_FDT/
- ATV320 DTM - Schneider_Electric_Altivar_Machine_ATV320_DTM_Library_V1.1.6
https://www.schneider-electric.com/en/download/document/ATV320_DTM_Library/
- ATV340 DTM - Schneider_Electric_Altivar_Machine_ATV340_DTM_Library_V1.2.3
https://www.schneider-electric.com/en/download/document/ATV340_DTM_LibraryEN/
- ATV6XX DTM - Schneider_Electric_Altivar_Process_ATV6xx_DTM_Library_V1.8.0
https://www.schneider-electric.com/en/download/document/ATV6xx_DTM_Library_EN/
- ATV9XX DTM - Schneider-Electric-Altivar-Process-ATV9xx-DTM-Library-V1.3.5
https://www.schneider-electric.com/en/download/document/ATV9xx_DTM_Library_EN/
- ATV32 / ATV71 / ATV61 / ATV LIFT / ATV31_312 / ATV212 / ATV12 AltivarDtmLibrary-V12.7.0
https://www.schneider-electric.com/en/download/document/Altivar_DTM_Library/

Acknowledgements

Schneider Electric would like to thank Haojun Hou from Adon for all the efforts related to identification and coordination of this vulnerability.

Important Security Notification

For More Information

This document is intended to help provide an overview of the identified situation 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 related to cybersecurity in Schneider Electric's products, please visit the company's cybersecurity web page:

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

THIS DOCUMENT IS INTENDED TO HELP PROVIDE AN OVERVIEW OF THE IDENTIFIED SITUATION AND MITIGATION ACTIONS AND IS NOT INTENDED AS A WARRANTY OR GUARANTEE OF ANY KIND, INCLUDING WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. THE USE OF THIS NOTIFICATION, INFORMATION CONTAINED HEREIN, OR MATERIALS LINKED TO IT ARE AT YOUR OWN RISK. WE RESERVE THE RIGHT TO UPDATE OR CHANGE THIS INFORMATION AT ANY TIME AND IN OUR SOLE DISCRETION.

About Schneider Electric

Schneider Electric is leading the Digital Transformation of Energy Management and Automation in Homes, Buildings, Data Centers, Infrastructure and Industries.

With global presence in over 100 countries, Schneider is the undisputable leader in Power Management – Medium Voltage, Low Voltage and Secure Power, and in Automation Systems. We provide integrated efficiency solutions, combining energy, automation and software.

In our global Ecosystem, we collaborate with the largest Partner, Integrator and Developer Community on our Open Platform to deliver real-time control and operational efficiency.

We believe that great people and partners make Schneider a great company and that our commitment to Innovation, Diversity and Sustainability ensures that Life Is On everywhere, for everyone and at every moment.

www.schneider-electric.com

Revision Control:

Version 1 <i>1 Mar 2018</i>	Original Release
---------------------------------------	------------------