

Schneider Electric Security Notification

ProClima (V1.1)

11 June 2019 (19 September 2019)

Overview

Schneider Electric is aware of multiple vulnerabilities in the ProClima product.

Affected Product(s)

All versions of ProClima prior to version 8.0.0

Vulnerability Details

CVE ID: **CVE-2019-6823**

CVSS v3.0 Base Score 8.8 | (High) | CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H

A CWE-94: Code Injection vulnerability exists which could allow an unauthenticated, remote attacker to execute arbitrary code on the targeted system.

CVE ID: **CVE-2019-6824**

CVSS v3.0 Base Score 9.8 | (High) | CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

A CWE-119: Buffer Errors vulnerability exists which allow an unauthenticated, remote attacker to execute arbitrary code on the targeted system

CVE ID: **CVE-2019-6825**

CVSS v3.0 Base Score 7.8 | (High) | CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H

A CWE-427: Uncontrolled Search Path Element vulnerability exists which could allow a malicious DLL file, with the same name of any resident DLLs inside the software installation, to execute arbitrary code.

Schneider Electric Security Notification

Remediation

These vulnerabilities are fixed in version 8.0.0 or higher and is available for download below:

<https://www.schneider-electric.com/en/product-range-download/2560-proclima/#tabs-top>

All previous versions should be upgraded to version 8.0.0 or higher.

Product Information

ProClima software processes a range of specified thermal data to propose the right thermal management choice to match the environment.

Product Category - Building and Automation Control

Learn more about Schneider Electric's product categories here: www.schneider-electric.us/en/all-products

How to determine if you are affected

Any version of ProClima prior to version 8.0.0.

General Security Recommendations

We strongly recommend following industry cybersecurity best practices such as:

- Locate control and safety system networks and remote devices behind firewalls, and isolate them from the business network.
- Physical controls should be in place so that no unauthorized person would have access to the ICS and safety controllers, peripheral equipment or the ICS and safety networks.
- All controllers should reside in locked cabinets and never be left in the "Program" mode.
- All programming software should be kept in locked cabinets and should never be connected to any network other than the network for the devices that it is intended.
- All methods of mobile data exchange with the isolated network such as CDs, USB drives, etc. should be scanned before use in the terminals or any node connected to these networks.
- Laptops that have connected to any other network besides the intended network should never be allowed to connect to the safety or control networks without proper sanitation.
- Minimize network exposure for all control system devices and/or systems, and ensure that they are not accessible from the Internet.
- When remote access is required, use secure methods, such as Virtual Private Networks (VPNs), recognizing that VPNs may have vulnerabilities and should be updated to the

Schneider Electric Security Notification

most current version available. Also recognize that VPN is only as secure as the connected devices.

Acknowledgements

Schneider Electric recognizes the following researcher(s) for identifying and helping to coordinate a response to this vulnerability:

CVE	Researcher(s) Name
CVE-2019-6823	Kushal Arvind Shah (Fortinet)
CVE-2019-6824	Telus
CVE-2019-6825	Haojun Hou Yongjun Liu (NSFOCUS security team)

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>

If you require additional support, Schneider Electric Industrial Cybersecurity Services team are available to help. Please visit: <https://www.schneider-electric.com/en/work/services/field-services/industrial-automation/industrial-cybersecurity/industrial-cybersecurity.jsp>

Legal Disclaimer

THIS DOCUMENT IS INTENDED TO HELP PROVIDE AN OVERVIEW OF THE IDENTIFIED SITUATION AND SUGGESTED MITIGATION ACTIONS, REMEDIATION, FIX, AND/OR GENERAL SECURITY RECOMMENDATIONS AND IS PROVIDED ON AN "AS-IS" BASIS WITHOUT WARRANTY OF ANY KIND. SCHNEIDER ELECTRIC DISCLAIMS ALL WARRANTIES, EITHER EXPRESS OR IMPLIED, INCLUDING WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. IN NO EVENT SHALL SCHNEIDER ELECTRIC BE LIABLE FOR ANY DAMAGES WHATSOEVER INCLUDING DIRECT, INDIRECT, INCIDENTAL, CONSEQUENTIAL, LOSS OF BUSINESS PROFITS OR SPECIAL DAMAGES, EVEN IF SCHNEIDER ELECTRIC HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. THE USE OF THIS NOTIFICATION, INFORMATION CONTAINED HEREIN, OR MATERIALS LINKED TO IT ARE AT YOUR OWN RISK. SCHNEIDER ELECTRIC RESERVES THE RIGHT TO UPDATE OR CHANGE THIS NOTIFICATION AT ANY TIME AND IN ITS SOLE DISCRETION.

Schneider Electric Security Notification

About Schneider Electric

At Schneider, we believe **access to energy and digital** is a basic human right. We empower all to **make the most of their energy and resources**, ensuring **Life Is On** everywhere, for everyone, at every moment.

We provide **energy and automation digital** solutions for **efficiency and sustainability**. We combine world-leading energy technologies, real-time automation, software and services into integrated solutions for Homes, Buildings, Data Centers, Infrastructure and Industries.

We are committed to unleash the infinite possibilities of an **open, global, innovative community** that is passionate about our **Meaningful Purpose, Inclusive and Empowered** values.

www.se.com

Revision Control:

Version 1 <i>11 Jun 2019</i>	Original Release
Version 1.2 <i>19 Sep 2019</i>	CVSS Base Score and Vector adjusted for CVE-2019-6823 and CVE-2019-6824 (page 1)