Schneider Electric Security Notification

PowerChute Business Edition

11 August 2020

Overview

Schneider Electric is aware of a vulnerability in the PowerChute Business Edition software which may lead to remote code execution.

Affected Product(s)

PowerChute Business Edition software V9.0.x and earlier

Vulnerability Details

CVE ID: **CVE-2020-7526**

CVSS v3.0 Base Score 7.1 | High | CVSS:3.0/AV:N/AC:H/PR:L/UI:R/S:U/C:H/I:H/A:H

A CWE-20: Improper Input Validation vulnerability exists which could cause remote code execution when a script is executed during a shutdown event.

Remediation

This vulnerability is fixed in version V9.1 and above. The latest versions are available for download below:

https://www.apc.com/pcbe

- Update to the latest release V10.x or above (64-bit environment) or V9.5 or above (32-bit environment)
- Reboot if required at the end of software installation.

The following workarounds and mitigations can be applied by customers to reduce the risk:

- Change user login password to a secure password.
- Utilize application whitelisting software.
- Utilize firewall rules to limit access to those intended to connect.

Schneider Electric Security Notification

Product Information

PowerChute Business Edition software provides UPS management, graceful shutdown and innovative energy management capabilities for servers and workstations using dedicated serial or USB connections.

Product Category - Critical Power, Cooling and Racks

Learn more about Schneider Electric's product categories here: https://www.se.com/us/en/all-products

How to determine if you are affected

Check the currently installed version in the Help > About menu. If V9.0.x or earlier, update to the latest version available on https://www.apc.com/pcbe.

General Security Recommendations

We strongly recommend the following industry cybersecurity best practices.

- Locate control and safety system networks and remote devices behind firewalls and isolate them from the business network.
- Install physical controls so no unauthorized personnel can access your industrial control and safety systems, components, peripheral equipment, and networks.
- Place all controllers in locked cabinets and never leave them in the "Program" mode.
- Never connect programming software to any network other than the network for the devices that it is intended for.
- Scan all methods of mobile data exchange with the isolated network such as CDs, USB drives, etc. before use in the terminals or any node connected to these networks.
- Never allow laptops that have connected to any other network besides the intended network to connect to the safety or control networks without proper sanitation.
- Minimize network exposure for all control system devices and 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). Recognize that VPNs may have vulnerabilities and should be updated to the most current version available. Also, understand that VPNs are 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-2020-7526	Mateus Riad

For More Information

This document provides an overview of the identified vulnerability or vulnerabilities and actions required to mitigate. For more details and assistance on how to protect your installation, please contact your local Schneider Electric representative and/or Schneider Electric Industrial Cybersecurity Services. These organizations will be fully aware of this situation and can support you through the process.

https://www.se.com/ww/en/work/support/cybersecurity/overview.jsp

https://www.se.com/ww/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.

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 *11 August 2020*	Original Release

Product Security Office Digitally signed by Product Security Office
Date: 2020.08.08 18:25:32 -04'00'