PowerChute™ Business Edition Security Features & Recommendations

By Chloe Conlon

ABSTRACT

PowerChute™ Business Edition software ships with APC-Smart UPS (5kVA and below) providing UPS management, graceful system shutdown and energy reporting using dedicated serial or USB connections.

This Application Note provides an overview of the security features in PowerChute including connectivity and authentication as well as recommendations on how to increase security for PowerChute.

Applications

Use PowerChute Business Edition software to gracefully shut down servers protected by an APC Smart-UPS in the event of an extended power outage.

Customer Benefits

- Graceful server shutdown
- Load shedding and scheduled shutdowns
- Energy reporting
- Event and data logging
- HTTPS communications
- IPv6 support

Introduction

All APC by Schneider Electric software products are developed in adherence with key security principles in order to deliver secure products protecting IT equipment.

This Application Note contains the following information:

- Connectivity
- Authentication
- Java Runtime Environment
- Configuration File Backup
- Vulnerability Reporting & Management
- Appendices
  - Security Hardening for PowerChute

APC by Schneider Electric

Connectivity

PowerChute Access

The PowerChute user interface is accessible via a web browser and supports TLS v1.2 which provides authentication and encrypted communication for sensitive communications.

If enabled and configured, PowerChute can be accessed via SNMPv1 or v3. It is recommended to use SNMPv3 as only this provides Authentication, Privacy and Access Control.

PowerChute supports MD5/SHA-1/SHA-2 for Authentication and DES/AES-128/AES-256 for Privacy when using SNMPv3.

PowerChute Business Edition provides secured browser access via HTTPS as default to ensure that communication via the web interface is secure and cannot be interpreted.

PowerChute uses a self-signed SSL Certification by default that has a 2048-bit RSA public key and uses the SHA-1 Signature Hash Algorithm.

Connectivity Protocol Definitions

Hypertext Transfer Protocol over Secure Socket Layer (HTTPS) is a Web protocol that encrypts and decrypts page requests from the user and the pages returned by the Web server.

Transport Layer Security (TLS) is a cryptographic protocol that provides communication security over the Internet.

Authentication

PowerChute User Interface

During PowerChute installation, you must enter a username and password that will be used to log on to the PowerChute UI.

Password Requirements

The password used for PowerChute must meet the following requirements:

- Minimum 8 and maximum 128 characters in length.
- One upper and lower case letter.
- One number or special character.

It is also advised to change the password on a regular basis e.g. every 90 days.

These credentials can be reset via the pcbeconfig.ini file.

User Control

The PowerChute session times out after 15 minutes of inactivity.

To ensure secure user control it is recommended that PowerChute is not available on a public-facing network segment.

©2018 Schneider Electric. All Rights Reserved. Schneider Electric and APC are trademarks owned by Schneider Electric Industries SAS or its affiliated companies. All other trademarks are property of their respective owners.

Java Runtime Environment (JRE)

JRE Utilization

PowerChute is shipped with an up-to-date private JRE as each new PowerChute version is released. PowerChute also allows you to upgrade your JRE using the Java Update tool in the PowerChute User Interface.

For more information on JRE versions included with and supported by PowerChute Business Edition, refer to the Operating System, Processor, JRE and Browser Compatibility Chart available on the APC website at: http://www.apc.com/wp/?um=100

Configuration File Backup

INI File

Some configuration settings, such as scheduled shutdowns, SNMP settings, and language settings, applied via the User Interface are stored on the local file system using the pcbeconfig.ini file. A backup of this file (pcbeconfig_backup.ini) is also stored.

User credentials are stored using the m11.cfg file and are encrypted. User credentials can be reset via the pcbeconfig.ini file. For more information, see the "General" section in the *PowerChute User Guide* available on the APC website.

Vulnerability Reporting & Management

How to report a Vulnerability

Cyber security incidents and potential vulnerabilities can be reported to Schneider Electric using the following link: https://www.schneider-electric.com/en/work/support/cybersecurity/report-an-incident.jsp

Security Updates and Notifications

Product Center Page

The Product Center page is accessible via the Help menu in the PowerChute UI and contains links to important Knowledge Base articles.

Update Notifications

If a security vulnerability is detected in PowerChute that requires a software update, a notification will be sent via the Update Notifications feature providing a web link from where the update can be downloaded. Software updates must be applied manually.

Knowledge Base

Security Bulletins in relation to known vulnerabilities are published on the Schneider Electric Knowledge Base.

©2018 Schneider Electric. All Rights Reserved. Schneider Electric and APC are trademarks owned by Schneider Electric Industries SAS or its affiliated companies. All other trademarks are property of their respective owners.

Appendix – Security Hardening for PowerChute

Recommended configuration changes to increase PowerChute security

1. Change the default password for the CACERTS keystore located below using the command: **keytool.exe -storepasswd -new -keystore cacerts -storepass changeit**.
    - **Windows:** C:\Program Files (x86)\APC\PowerChute Business Edition\jre\lib\security\cacerts
    - **Linux:** opt/APC/PowerChuteBusinessEdition/jre/lib/security/cacerts
2. Ensure that the file permissions set for the **jre** folder and its contents allow read/write access only for trusted users and LocalSystem account on Windows and root account on Linux/Unix.
3. Prevent Remote Access to the Web UI if this is not required using a firewall rule for TCP port 6547. To prevent Denial of Service attacks such as the SSL THC DOS attack these ports should be blocked and we do not recommend allowing access to PowerChute on a public facing network interface.
4. If the JRE used by PowerChute is changed via the Java Update tool, the JRE should be updated regularly as software updates and security fixes are released.
5. If using SNMP with PowerChute, it is recommended to only use SNMP v3 and to choose SHA-2 and AES128 or higher for Authentication and Privacy. Please refer to APC Knowledge Base Article FA290630 for more information on how to enable support for AES-192 and AES-256. Access Control should also be configured to restrict access to PowerChute via SNMP.

©2018 Schneider Electric. All Rights Reserved. Schneider Electric and APC are trademarks owned by Schneider Electric Industries SAS or its affiliated companies. All other trademarks are property of their respective owners.