# Security Questionnaire

|  |  |
| --- | --- |
| Manufacturer |  Grid Protection Alliance |
| Model | openPDC |
| Vendor Sales Engineer | Erika Wills |
| Vendor Sales Contact Info (Email/Phone) | elwills@GridProtectionalliance.org |
| Date Information Provided | 10/13/2023 |

## Ports & Services

1. Which ports and services are enabled by default when the device is shipped?

No Device is shipped. Product is Software application.

|  |  |  |
| --- | --- | --- |
| **Service** | **Protocol** | **openPDC** |
| **Primary Web Interface** | http | 8280 |
| **Service Console Access** | tsf-ssr\* | 8500 |
| **Alarm Data Webservice** | http | 5018 |
| **PPA Metadata Webservice** | http | 6151 |
| **PPA Time-series Webservice** | http | 6152 |
| **PPA Grafana API** | http | 6452 |
| **STAT Metadata Webservice** | http | 6051 |
| **STAT Time-series Webservice** | http | 6052 |
| **STAT Grafana API** | http | 6352 |
| **STTP** | sttp | 7165 |
| **STTPS** | sttp | 7167 |
| **GEP (Internal)** | gep | 6165 |
| **GEP (External)** | gep | 6156 |
| **GEP (TLS)** | gep | 6167 |

1. What is the process for disabling ports and services?

Depends on the specific service/port, but all services can be disabled either via changes to the application configuration file or using the build in user interfaces.

1. Are there any ports or services, which cannot be disabled?

All services can be disabled; However, this may impact functionality required by this project.

1. Can someone port scan the device?

Yes.

1. What is the recommendation when port scanning the device? Are there any specific ports to avoid?

GPA recommends scanning all ports on the system for vulnerabilities.

## Security Patch Management

1. How often do you release software patches?

GPA releases patches on an as needed basis.

1. What’s the procedure/process for implementing these patches?

Patches usually come in the form of one or more assembly files that replace existing files in the installation folder. A standard MSI file may be available if needed.

1. How do you analyze, research/test, plan, deploy, and back out patches if necessary?

We track a combination of version numbers, change logs, and code branches to determine which out-of-cycle patches were deployed to each individual client. This allows us to target the specific version of the codebase is being used by the client along with any patches that have already been delivered and continue to add patches for that version. If patches need to be backed out or revised, we can adjust based on the information in the change log or code branch we use to track it.

1. Can patches be applied without interrupting proper operation of the device? If reboots or other interruptions are required can they be delayed or scheduled to occur at a specific time in the future?

The software will need to be interrupted in order to apply the patch. This is a manual process and can therefore easily be scheduled by the person performing the work.

1. If critical patches get released, how quickly can you certify this patch and get communication out to customers?

If a major security flaw requiring a critical patch is discovered GPA communicates this need within 24 hours of the patch being available.

1. Can you patch across the network or does user have to be on the device?

Patches can be applied across the network via standard windows remoting software such as RDP or WMI

1. How do you respond to vulnerability reports?

GPA reviews vulnerability reports for potential exploitation of these vulnerabilities in our software. Regardless of whether we determine if a vulnerability can be exploited, GPA follows recommendations to update references to third-party dependencies. If the vulnerability can be exploited, GPA will provide details to clients and recommend software updates or workarounds to mitigate the vulnerability.

## Malicious Software Prevention

1. Does the device support anti-virus or malware prevention tools? If so, please describe in general terms (e.g. Signature Based A/V, Behavior Based, Application White listing, etc.)

They are supported. However, some of the more heavy-handed anti-malware policies have been known to filter our upgrades and/or patches for reasons similar to the following:

1. The scanner found Mark of the Web on an assembly once and can no longer be convinced to trust it.
2. There are not enough users of the anti-virus software who have indicated that our application is trustworthy.
3. How will your application respond to scanning tools such as Nessus, HFNetCheck, etc and antivirus?

The application will run as normal, provided that the scanner does not quarantine any of the files used by it.

1. Other than anti-virus or malware prevention what methods or practices does the vendor recommend to mitigate risk exposure?

Review of Windows security patches and keeping the OS up to date.

1. Does the vendor provide to or notify customers of updated anti-virus and malware prevention signatures applicable to the device?

No.

## Account Management

1. Does the device support individualized accounts and passwords?

Yes. The software supports integration with Windows AD, Windows Azure Active Directory and local credentials stored encrypted in the applications database.

1. How many accounts can be created?

No Limit.

1. Are the passwords user-modifiable?

Yes.

1. What is the minimum number of characters in a password?

Configurable (8 by default).

1. What characters are required or allowable in creating a password?

Configurable (at least one uppercase letter, at least one lowercase letter, and at least one number is required by default).

1. Are users required to change password periodically? If yes, what is the time period?

Configurable (default every 90 days).

1. What is the method for removing, disabling, or renaming accounts?

Users are managed through the user interface. Windows or Azure integration manages users via the AD.

1. Are there any accounts which cannot be deleted? If yes, are the passwords re-settable?

No.

1. Is there an account lockout after X amount of failed login attempts?

No.

1. What user account information is logged when the device is accessed?

The system stores the username and whether the authentication was successful.

1. Does the device support syslog?

The application does not directly support syslog, but it does send logs to the windows eventlog.

1. Does the device support SNMP

The application does not directly support SNMP.

1. What logs can be accessed locally?

The application maintains it own text files for logging errors and informational messages from the service, detailed status of modules loaded into the application, and health statistics sampled from Windows Performance Counters.

1. What is the maximum number of entries in the access logs?

Configurable via Windows.

## Security Status Monitoring

1. What capabilities does the device possess for monitoring and detecting cyber security incidents?

The application does not support this type of monitoring.

1. Does the device have the capability to issue alerts if incidents related to security are detected?

No. Cyber Security incidents will not be detected.

## Disposal or Redeployment

1. What is the policy regarding critical cyber assets returned to vendor for repair?

N/A

## Other

1. Does the device use a publicly recognized, general-purpose operating system (Windows, MS-DOS, Linux, UNIX and “UNIX-like”, Apple/Macintosh)?

The application runs on Windows.

1. For applications to be loaded on device:
	1. List the account/identity and privileges under which applications must run

For the services:

1. GMSAs are recommended.
2. The account needs read/write permissions to the installation directory.
3. For performance logging the account needs to be added to the Performance Log Users and Performance Monitor Users groups.
4. The account needs permission to start and stop the service.
5. The account needs read/write access to the applications database.

For the Console and management applications:

1. These applications are run as the user that launches them using non-elevated privileges.
2. The user running these applications may need read/write access to the applications database.
	1. List the ability of the application to change the configuration of the device

The application may update the database or its own configuration files based on user input or automated processes.

* 1. List the ability of the application to remove/install additional software

The application should not be allowed to remove or install additional software.

1. Is the device capable of routing IP traffic? If so, can IP routing be disabled?

Other than internally routing its own traffic the application is not capable of routing.

1. Does the device have a wireless interface? If so, can it be disabled?

N/A

1. Does the device support DHCP? If so, what options are supported?

N/A