Cybersecurity Best Practices for Embedded Software

Rev B | Feb 2024

VOLTSERVER
DIGITAL ELECTRICITY™

Cybersecurity Best Practices for Embedded Software

Cybersecurity is dependent on numerous factors, including threat model, physical environment, and the network environment where the product resides. As such, this guide is not meant to be exhaustive but a baseline of cybersecurity best practices for VoltServer products in deployed environments.

Scope

This Application Note applies to VoltServer Transmitter "E" model chassis that supports MGT500E management cards and SW. The transmitters in this population include VoltServer PTX500E-DC, PCX500E-AC-0x, and ETX8-SA. White-label versions of these products are also within the scope of this Application Note.

Features described within this application note may vary with system SW versions lower than v1.9.2, which is the current production release as of the latest revision of this document.

Basic Network Architecture

The VoltServer Transmitter chassis serves as a basic Network Element (NE) endpoint within a managed network. Multiple NEs are connected to Local Area Network (LAN) switch ports to aggregate traffic for connection to the network router. The router/gateway may, in turn, be connected to the Wide Area Network (WAN), which manages traffic between the Public Internet and the Local Private sides of the network.

Checklist of Practices

- ✓ Controlled access to NE
- ✓ Change the default admin password
- ✓ Use RADIUS
- ✓ Assign appropriate user roles (for local user accounts and using RADIUS **Filter-Id** attribute)
- ✓ Keep devices behind a network firewall
- ✓ Use VLAN/ network isolation

Controlled Access Space

The VoltServer Transmitter is designed to be placed within a Controlled Access Space (CAS) for both electrical safety and network security purposes. The CAS prevents unauthorized personnel from accessing electrical connections, removal of cards, and gaining access to the LAN side of the network.

User Authorization

Change the default admin password to a strong, unique password. Record and manage the credentials according to your cybersecurity policy.

RADIUS

Enable RADIUS on the device and use a RADIUS server to manage user access. This eliminates the need for shared passwords for device access.

User Roles

Create/manage users with the appropriate level of access by role assignment. In general, “Basic” users are read-only, and “operator” users may perform some functions such as managing email alerts and DE channel output power. “Admin” users have access to all settings including creating and deleting other local user accounts. For full details on role access, see the Software Feature Guide.

For RADIUS users, the role is determined by the **Filter-Id** value sent in the **Access-Accept** response. Valid **Filter-Id** values are detailed in the Software Feature Guide.

Network

VoltServer products should be on a secure, trusted LAN behind a network firewall. Use a VPN if remote access is needed for monitoring or management. Avoid putting VoltServer products on a public, Internet-facing IP.

HTTPS

The NE may be accessed via HTTPS. The device uses a self-signed certificate, which will induce an “untrusted certificate” prompt the first time the user opens the device webpage. If the user chooses to trust the certificate, subsequent traffic will be encrypted using TLS 1.2.

Network Isolation

VoltServer equipment on a private network should be completely isolated, i.e., using VLAN or other method such that each device only has access to the services needed for it to operate. Devices do not need to communicate with each other. The following is a list of services that the device may need access to: