DFS Maintenance, Software & Security

Covenant Document

December 12, 2021

Contents

1. DFS Commitment:

1.1. DFS Responsibility:

1.1.1. Installing and testing the latest Debian security updates for our Server Debian Linux OS at least once per quarter **until the current Debian distribution reaches EOL (usually about 3-4 years).**

1.1.2. Ensuring that no malware, virus, or known-security vulnerabilities exist within any software update package distributed to customer systems or for customer use. The scope includes Module firmware update binaries, TCU/RDP/PLC USB Updates, HT4 Server update packages, and Software Tools (WinRTU, PMT, etc.)

1.1.3. Ensuring any laptop or computer hardware delivered or sold with the system is free from malicious software **at the time of hand-off.**

1.1.4. Provide documentation for properly and safely updating their system via acceptable methods, including USB updates for TCU/PLC/RDP devices.

1.1.5. Assisting customer IT departments with troubleshooting network issues related to our system **when requested**.

1.1.6. Provide a functional software firewall on Debian Linux-based OS systems **if requested**. DFS **must** be involved with the setup of this firewall.

1.1.7. Providing customer login credentials for the Debian Linux OS if DFS relinquishes the responsibility for maintaining and updating their system, or otherwise cannot due to the system's lack of access or age (i.e., Debian distribution is too old to receive updates).

1.2. DFS Maintenance responsibilities:

1.2.1. <u>General Maintenance</u>

1.2.1.1. We ensure customers are aware of our access to their system and can monitor any changes we make to their Debian Linux OS.

1.2.1.2. We apply the latest Debian Linux OS security updates to all our applicable products **when customers request them.** Requires at **least one months' notice** and **remote VPN access to the network their system resides**.

1.2.1.3. We apply the latest firmware update to customer RTU Modules or TCU/RDP/PLC **when customers request them**. Updates require at **least one months' notice and appropriate access to the specific device.**

1.2.1.4. When we remotely access customer networks, we ensure (through security best practices) we do not expose the customer's network to any malware, virus, or other malicious software that would otherwise harm or compromise their network's integrity.

1.2.1.5. We manage and maintain the cellular access and security to customers' Cellular RTUs by working with Verizon (subject to change).

1.2.2. <u>Routine Maintenance</u>

1.2.2.1. DFS performs no routine maintenance unless requested to do so by the customer.

1.2.2.2. DFS conducts unsolicited informational warnings with follow through on corrective action whenever DFS discovers a threat that may compromise or provide a vulnerability to the DFS hardware or software.

2. End-User / Customer Commitment:

2.1. End-User / Customer Responsibility:

2.1.1. Updating and maintaining security updates on any Debian Linux OS-based system that **DFS cannot remotely or physically access**.

2.1.2. Ensuring that no malware, virus, or otherwise harmful software is added to the software packages we provide **after** being downloaded from our website or to the USB that we may ship with software updates.

2.1.3. Ensuring that no malicious devices exist on the radio frequency the customer has licensed to themselves.

2.1.4. Only allowing DFS remote access when DFS explicitly requests it. Verifying the individual requesting access is a valid DFS employee and not a potential imposter.

2.1.5. Providing and managing a physical firewall maintained by a **trusted IT department** to protect our Debian Linux OS-based (applies to HSM server only).

2.1.6. Ensuring that radio hardware (i.e., cellular modem, radio modules, etc.) is NOT disassembled or swapped from their module boards unless performed by a DFS repair technician, an authorized VAR, or with the explicit approval of DFS.

2.2. End-User / Customer Maintenance Responsibilities:

2.2.1. General Maintenance

2.2.1.1. Contacting DFS to either: (1) ask for an update to be applied, or (2) ask for assistance in applying an update that is provided in the form of a package (i.e., USB, zip file, etc.)

2.2.1.2. Report any anomalies within the SCADA System.

2.2.1.3. Protect all DFS equipment (hardware and software) from physical or remote access by any unauthorized user.

2.2.1.4. Maintain best security practices with computers/laptops connected to DFS devices via a network, ensuring no malware, viruses, or otherwise harmful software can compromise our software.

2.2.2. Routine Maintenance

2.2.2.1. Schedule Lifecycle Maintenance (SLM) is the DFS prescribed maintenance program for the DFS Systems. The SLM covers a detailed training program and written procedures available from DFS. SLM is comprehensive and expansive in providing basic expected maintenance practices. However, it extends further by addressing complex maintenance actions requiring technician-level expertise.

2.2.2.2. Training in the SLM is available to all DFS customers. In addition, DFS provides opportunities for free training at our facility throughout the year, when available (seating has restrictions and space is limited) in differing aspects of the customers' SCADA system maintenance. The maintenance program training at the customers' location is available via service purchasing.

3. Additional Information of Note:

3.1. Usual Expected Method for customer System Access to SCADA:

3.1.1. HSM (HT4 Server)

3.1.1.1. Webserver (Apache, HTTPS) using the provided HT4 interface.

3.1.1.1.1. DFS provides customer default login.

3.1.1.1.2. Customers can create their logins and access accounts to the system.

3.1.2. RTU Smart Devices (Network capable, PLC800 and RTU local HMI)

3.1.2.1. LAN Access via direct connection with a laptop.

3.1.2.2. Access telemetry points via HT4 Server (after login authentication).

3.2. DFS Provided System Software:

3.2.1. Module Firmware

3.2.1.1. Firmware can be modified via "firmware update" from HT4.

3.2.1.1.1. The procedure requires DFS service involvement.

3.2.2. PLC/RDP/TCU800 Debian Linux OS

3.2.2.1. Updates to TCU800 are via USB with an update package provided by DFS.

3.2.2.2. Updates to PLC800 and RDP800 are via a special firmware upgrade that DFS prepares by request (for emergency updates only).

3.2.3. Server (HT4 and HSM Debian Linux OS)

3.2.3.1. Updates can be modified via DFS-prepared update packages and require DFS involvement.

3.2.3.2. Debian Linux OS is effectively isolated from the customer interface.

3.2.4. Tools (WinRTU, PMT)

3.2.4.1. Both are tools used to update firmware or automation programming of field devices with updates prepared by DFS

3.3. RTU Radio and Cellular Communications Network Information

3.3.1. Our cellular devices are on a private network and cannot be directly accessed from the world-wide-web. Furthermore, their addresses are statically defined and must be known when activated.

3.3.2. Cellular comm is encrypted by default. Radio comm can be encrypted **if requested**, but by default is **not.**

3.3.3. We can provide a list of open ports if requested.