How Does DFS Stay Secure?

All “smart” DFS products run an operating system called Debian, a distribution of the open source Linux kernel. A list of these products include:

- HSM
- TCU800
- RDP
- PLC800

We have chosen Debian because of its reputation and excellent support. Debian is comprised of many major software releases, with each one having its own name, lifetime of support, and security updates. The Product Engineering team works hard to ensure our current supported software is always within the current Debian lifetime.

For a full list of DFS security practices and policies, it is recommended to review the *DFS Maintenance, Software & Security Covenant Document***.** This document outlines DFS and customer responsibilities to keeping a secure system.

The Future of HT3 and Wheezy

Our HT3 interface runs on the release of Debian called Wheezy who reached its End of Life on July 18th, 2020, but has had Extended Long Term Service to June 30th, 2027. Extended Long Term Service is not an official service offered by the Debian organization, but by a third party. So support is not guaranteed. Due to these factors, the age of the release and its 32-bit architecture, it is no longer viable or possible to ensure quality feature or security updates for our HT3 systems.

HT 4.0.13, released December of 2022, is the last feature update for HT3 Wheezy systems. HT3 Wheezy systems will continue to get bug fix updates throughout 2023. There will be no new features back-ported to HT3, all future software features will exist only on current supported HyperTAC software.

HT3 Wheezy systems will officially stop receiving updates by the end of 2023. It is highly advised that any customer still running this version of software to immediately update to our current HT4 release, running Debian Buster. System updates can be scheduled with our Service department.

How Can I Ensure I’m Protected?

There is no one answer to this question, however there are many steps you can take to ensure your DFS system is best protected from attacks.

1. Always keep your DFS products software up to date.
2. Ensure passwords and other virtual access to DFS products are protected.

3. Ensure your DFS products have appropriate physical security. This includes locking entry to products and managing employee access.
4. It is strongly recommended to install an HSM in a network managed by a physical firewall. Each HSM also comes with a software firewall. DFS **must** be consulted with any firewall configuration to ensure product compatibility.
5. It is **never** approved or advised to make an HSM publicly accessible from the internet. If such accessibility is required, using a password protected VPN or other tunneling method is advised.

For a detailed list of the Debian packages and libraries installed on our latest supported software updates, documentation can be provided if **requested** to the Service department.

What About Major Vulnerabilites?

Each security update is assigned a CVE number, assigned by the CVE program. The CVE number is determined by the following factors:

- Access vector
- Attack complexity
- Authentication
- Confidentiality
- Integrity
- Availability

This program, which stands for Common Vulnerabilities and Exposures, is used by the U.S. National Vulnerability Database and is the main driving force behind all of our software security decisions at DFS. The scale is on a 0.1-10.0 severity scale with Low being on the less severe side and Critical being on the most severe side. On average, most if not all annual CVE reports fall in the Low and Medium categories.

It is our policy for all High reports that affect our system to review the vulnerability and patch on an as needed basis. These updates will come out during the quarterly bug update or next schedule update for current supported software.

It is our policy for all Critical reports that affect our system to immediately inform customers and produce an unscheduled update for current supported software. These updates have happened before with Log4j and OpenSSL vulnerabilities.

Contacting the DFS Service Department

For any questions and concerns, our Service department can be contacted by phone or email Monday through Friday from 8am-5pm EST. Our phone number is 321-259-5009 x1117, and our email is service@dataflowsys.com.