TELEDYNE | Teledyne LABS

PeakTrak Security

keywords: chromatography, PeakTrak, software, networking

Teledyne LABS monitors the evolving cybersecurity landscape and considers the impact on its products and customers to best mitigate or address concerns.

Teledyne LABS chromatography products use PeakTrak software for system control. Each product uses a customized version of PeakTrak to implement capabilities unique to the system while still sharing many features. PeakTrak software is designed to operate with a Linux operating system, which is also customized for the instrument.

Each system ships with a version of Linux that was contemporary at the time the system was launched, resulting in several versions of Linux in use among different systems. The Torrent and EZ Prep instruments have had multiple operating system versions as their motherboards became obsolete and were replaced with newer versions that required new operating systems. The original motherboards are not supported by the new operating systems, so if an operating system update is needed, a new motherboard is required. The ACCQ*Prep* HP125 and HP150 systems have been upgraded for improved security and compatibility. Their motherboards remain unchanged. Other instrument models have not had any operating system upgrades.

Teledyne LABS regularly releases software updates (improved features or functionality and bug fixes) free of charge to the customer; these software updates typically only update the internal PeakTrak application, not the operating system, SSH, or Apache. On a case-by-case basis, in response to security concerns or other needs, Teledyne LABS will release updates that could include updates to the OS, kernel version, Apache version, or OpenSSH version.

Instrument	Operating System	Kernel Version	Apache Version	OpenSSH Version
Torrent (Operating System 2)	CentOS Linux 6.5	2.6.32	2.2.15	5.3p1
Torrent (Operating System 4)	CentOS Stream 9	5.14.0	2.4.53	8.7p1
EZ Prep (Operating System 2)	CentOS Linux 6.5	2.6.32	2.2.15	5.3p1
EZ Prep (Operating System 4)	CentOS Stream 9	5.14.0	2.4.53	8.7p1
ACCQ*Prep* HP125 / HP150 (Operating System 2)	CentOS Linux 6.5	4.4.17	2.2.15	5.3p1
ACCQ*Prep* HP125 / HP150 (Operating System 4)	CentOS Stream 9	5.14.0	2.4.53	8.7p1
ACCQ*Prep* SFC	CentOS Stream 9	5.14.0	2.4.53	8.7p1
Combi*Flash* NextGen	CentOS Linux 7	3.10.0	2.4.6	7.4p1

Network Security considerations

- We recommend that the instrument be placed behind a firewall and that it not have a public, routable IP address.
- The installed Linux version has had all nonessential components removed. An Apache web server operating internally functions as an intermediary between the operating program and the user interface portions of the instrument.
- The only services running on the instrument are HTTP (port 80) and, on most instruments, SSH (port 22). ACCQ*Prep* HP125/HP150 version 4.3.25 and newer and ACCQ*Prep* SFC 6.1.4 and newer have the SSH service disabled by default. It can be enabled temporarily by service personnel if needed. All other models and versions have it enabled without the possibility of disabling it
- The Apache HTTP server is used to communicate with the client software, and the SSH is available for maintenance. By default, the instrument does not attempt to directly access the internet or any other computer; it only responds to requests from outside computers. It will access outside servers in a few cases when features are configured and turned on.
  - The instrument will access user configured servers when the network file save feature is enabled by the user.
  - The instrument will access user configured time servers when automatic time synchronization is enabled by the user.
  - The instrument will access user configured printers if this feature is enabled by the user.
- The instrument does not support HTTPS (encrypted) connections. While the results are important, they do not require the same level of security that something like a credit card number would require. By placing the instrument behind a firewall, only computers on the local network would be able to snoop on the traffic, and these are assumed to be trusted.
- The instrument has no anti-virus software. Due to the limited services running and if it is located behind a firewall as recommended, network worms pose little threat. Because the instrument is not used for general web browsing or email, there is no chance of the user accidentally downloading a virus to the instrument.
- As an additional level of security, the hard drive is configured so that the operating system is installed on a read-only partition, and a separate partition is used for storing the data files. This prevents the operating system files from being accidentally or intentionally corrupted and prevents software from being installed.
- Software updates are scanned for viruses by Teledyne LABS before release to customers.