Dallmeier

REV. 1.0.0 | 2021-08-26

WHITEPAPER

BASIC INFORMATION

SYSTEM SECURITY

METHODS TO ENSURE THE INTEGRITY OF THE LINUX OPERATING SYSTEM AND THE INTEGRATED 3RD PARTY SOFTWARE.

MADE IN GERMANY

See more.

The manufacturer accepts no liability for damage to property or pecuniary damages arising due to minor defects of the product or documentation, e.g. print or spelling errors, and for those not caused by intention or gross negligence of the manufacturer.

Figures in this document may differ from the actual product.
Specifications subject to change without notice. Errors and misprints excepted.

1 ABSTRACT

Dallmeier products are thoroughly tested prior to shipment in order to ensure a maximum security and integrity of the systems. As early as in the development stage of the integrated software, highest priority is given to the security of the underlying Linux operating system and the integrated 3rd party software.

This document contains a general description of the methods for securing the integrity of the Linux operating system and the integrated 3rd party software.

2 VALIDITY

This document applies to Dallmeier recording systems V8, V9, V10.

3 SECURITY PRECAUTIONS

Secure operating system
Dallmeier recording systems are equipped with a highly adjusted and hardened Linux operating system. Compared to other operating systems, this provides significantly enhanced security in case of attacks and higher system stability.

Proprietary file system
Dallmeier recording systems use a proprietary method of data storage with separated and decentralised keeping of data. Image data cannot be recognized as such and cannot be evaluated even if the storage medium is copied.

Integrated software modules and services
In all cases, only absolutely necessary software modules are integrated into Dallmeier recording systems. Additionally, unnecessary standard services were removed during the adjustment of the operating system.

Deactivation of services and ports
Unused ports are closed by default. The few integrated services and the ports used by them can be deactivated via the graphic configuration interface. We recommend the deactivation of all redundant services and ports during the system integration.

Fail2Ban function
Dallmeier recording systems have a Fail2Ban function for monitoring of login attempts over the network. After 10 login attempts with incorrect user name or password, the IP address of the accessing client is blocked for 10 minutes.

No software installation

Dallmeier recording systems do not offer any possibility to start or install software from a connected medium. Also, the start from a connected or integrated drive is prevented by default through an appropriate configuration of the password protected BIOS.

User administration

Dallmeier recording systems are equipped with a detailed user administration, which is separated from the operating system. User rights can be defined individually and in detail in order to prevent sabotage or misuse of the data.

Encrypted transmission

For the connection to clients, Dallmeier recording systems have functions for the encrypted transmission of user names and passwords to effectively prevent sniffing attacks on the network.

Secure remote configuration

Dallmeier recording systems can be configured directly (monitor and mouse) or with the software NetConfig3 over the network. If a direct configuration is active, the remote configuration is blocked. Thus a spying of settings or data (e.g. passwords) is to prevent.
In addition, the recording system can be set to accept a remote configuration only from a client who has a special dongle.

4 MEASURES

Monitoring and updating

The Dallmeier quality assurance is continuously monitoring external notifications and news groups featuring reports about potential weaknesses of the integrated 3rd party and the underlying Linux operating system that could be exploited for an attack. Suitable up-to-date versions of the 3rd party software are incorporated into the latest, and normally cost-free, updates. With these security measure of course only currently existing weakness can be remedied. Additionally, the software offers various possibilities (port locking) to ensure system and data security in case new danger points should emerge.

Analysis and adjustment

Should the above-mentioned security precautions and measures not provide sufficient protection and should new weaknesses allow for a successful attack on a correctly configured system, we guarantee that we will analyze the problem and provide an optimized update.

5 ANTI VIRUS PROTECTION

All Dallmeier products are thoroughly tested before they are dispatched to eliminate virus infections as far as possible. During software development, for example, up-to-date virus scanners are in permanent use to check the software products for any possible infection with viruses. However, since all such measures of protection only cover those viruses that are already known and no one can predict the way in which computer viruses will develop in the future, the protection offered can never be more than relative.

However, we offer our assurance that we shall continue to take on board new developments in anti-virus protection in future and – where feasible – use them for our devices to minimize the residual risk that can never be fully eliminated.

Currently the following security precautions are taken against infection by viruses:

Linux operating system
The most important security measure for Dallmeier products is the use of the Linux operating system. This measure has led to a significant reduction in the current risk of infection by a virus because this operating system is far less susceptible to viruses than other any other system. At the same time it is impossible to predict the way in which computer viruses which may affect Linux will develop in future, which means this statement only applies to the position as it stands at present.

Separated network (DMZ)
Even the use of the Linux operating system cannot eliminate the possibility of infection by currently unknown pests as soon as the devices are open to general access via the Internet. Security against such attacks from the Internet is largely dependent on the network structure and network configuration in which the Dallmeier product is embedded. Generally, independent from a thread from malware, we recommend to operate recording systems and cameras in specially constructed networks (DMZ) with a upstream firewall and to deactivate all not necessary services on the device itself.

Anti-virus software
Products that work exclusively with pre-installed windows operating systems (workstations) are shipped by us without pre-installed anti-virus software. We strongly recommend to license and install a suitable anti-virus software (current recommendation: Sophos).
For products that work exclusively with Linux (cameras and recording systems) an installation of an anti-virus software is not required and will lead to disturbance of the correct operation.

[THIS PAGE WAS INTENTIONALLY LEFT BLANK]

[THIS PAGE WAS INTENTIONALLY LEFT BLANK]

HEAD & ACCOUNTS OFFICE

Dallmeier electronic GmbH & Co.KG
Bahnhofstr. 16
93047 Regensburg
Germany

tel +49 941 8700 0
fax +49 941 8700 180
mail info@dallmeier.com

www.dallmeier.com