Security Advisory Polkit pkexec

Polkit is an authorization service on Linux operating systems that allows communication between user software and system components if appropriate privileges are set. A vulnerability (CVE-2021-4034) was discovered in the included component **pkexec**, which allows local privilege escalation and thus the acquisition of root privileges.

PolKit is installed on almost all Linux distributions. The systems are vulnerable even if the package is merely installed and the PolKit daemon is not running. However, exploiting the vulnerability requires local access to the system.

No Endangerment

Dallmeier has already reviewed all recording systems, cameras as well as software products regarding the Polkit pkexec vulnerability. A Linux operating system with the **Polkit pkexec** component **is not used** in the following products. There is **no risk** to these products from exploitation of this vulnerability.

- All network cameras
- All recording systems
- Panomera® Streaming Server
- CAT Server
- External AI Server
- SeMSy® Compact
- SMAVIA Viewing Client
- PService3
- Dallmeier Device Manager
- DMVC 2 Server
- DMVC 2 Apps (iOS, Android)
- SeMSy® III Video Management System

Endangerment

Dallmeier experts have identified the **vulnerability** in the Ubuntu distribution, which is used as a component in the **HEMISPHERE® Backbone Server software**. All **versions up to 0.3.9** are affected. Version 0.3.9 and following will be delivered with a corresponding patch from Canonical.

Procedure

For previous versions of the **HEMISPHERE® Backbone Server Software**, Dallmeier's experts have already developed an immediately available **solution to fix the vulnerability**. The **hot-fix package** contains the patch from Canonical as well as updates for other connected components. The installation of the hot fix package can be done remotely and during operation.

The HEMISPHERE® Backbone Server Software is exclusively **used in projects** that are **directly supported by Dallmeier experts**. The corresponding contact persons of the **project teams will proactively approach affected customers and partners** and **coordinate the implementation of the adjustments**. In addition, they will be available for any inquiries, just like the contact persons of the sales teams.

General Endangerment

Note that due to the **use of Polkit in all Linux distributions**, a large number of devices and applications are at risk from the **pkexec vulnerability**. Apart from Dallmeier components, **all other components of a video system** are thus potentially at risk, such as:

- Servers
- Routers and switches
- Virtual systems
- 3rd party network cameras

Dallmeier products and third-party products purchased through Dallmeier are always delivered with the latest updates and security patches at the time of shipment.

At present, corresponding updates and patches are already offered. If necessary, note the current information from the relevant manufacturers.