Security Advisory Polkit pkexec

Polkit ist ein Berechtigungsdienst auf Linux-Betriebssystemen, der eine Kommunikation zwischen Benutzersoftware und Systemkomponenten erlaubt, wenn entsprechende Berechtigungen eingerichtet sind. In der enthaltenen Komponente **pkexec** wurde eine Schwachstelle (CVE-2021-4034) entdeckt, die eine Rechteausweitung (Local Privilege Escalation) und damit das Erlangen von Root-Rechten erlaubt.

PolKit ist auf fast allen Linux-Distributionen installiert. Die Systeme sind auch dann verwundbar, wenn das Paket lediglich installiert ist und der PolKit-Daemon nicht ausgeführt wird. Das Ausnutzen der Sicherheitslücke erfordert allerdings lokalen Zugriff auf das System.

Keine Gefährdung

Dallmeier hat bereits alle Aufzeichnungssysteme, Kameras sowie Software-Produkte bezüglich der Polkit pkexec Schwachstelle überprüft. Ein Linux-Betriebssystem mit der Komponente **Polkit pkexec** wird in den folgenden Produkten **nicht eingesetzt**. Für diese Produkte besteht **keine Gefährdung** durch eine Ausnutzung dieser Schwachstelle.

- Alle Netzwerkkameras
- Alle Aufzeichnungssysteme
- Panomera® Streaming Server
- CAT Server
- Externe AI Server
- SeMSy® Compact
- SMAVIA Viewing Client
- PService3
- Dallmeier Device Manager
- DMVC 2 Server
- DMVC 2 Apps (iOS, Android)
- SeMSy® III Video Management System

Gefährdung

Die Experten von Dallmeier haben **die Schwachstelle** in der Ubuntu-Distribution festgestellt, die als Komponente in der **HEMISPHERE® Backbone Server Software** eingesetzt wird. Betroffen sind alle **Versionen bis 0.3.9**. Version 0.3.9 und folgende werden mit einem entsprechenden Patch von Canonical ausgeliefert.

Maßnahmen

Für frühere Versionen der **HEMISPHERE® Backbone Server Software** haben die Experten von Dallmeier bereits eine **sofort verfügbare Lösung zur Behebung der Schwachstelle** erarbeitet. Das **Hot-Fix-Paket** enthält das Patch von Canonical sowie Updates für weitere angeschlossene Komponenten. Die Installation des Hot-Fix-Paketes kann remote und im laufenden Betrieb vorgenommen werden.

Die HEMISPHERE® Backbone Server Software wird ausnahmslos **in Projekten eingesetzt**, die **direkt von Experten von Dallmeier betreut** werden. Die entsprechenden Ansprechpartner der **Projektteams werden proaktiv auf betroffene Kunden und Partner** zugehen und die **Durchführung der Anpassungen koordinieren**. Daneben stehen sie ebenso wie die Ansprechpartner der Salesteams für etwaige Nachfragen zur Verfügung.

Allgemeine Gefährdung

Beachten Sie, dass durch den **Einsatz von Polkit in allen Linux-Distributionen** eine Vielzahl von Geräten und Anwendungen durch die **pkexec Schwachstelle** gefährdet sind. Abgesehen von Dallmeier Komponenten sind damit **alle weiteren Komponenten eines Videosystems** potentiell gefährdet, wie beispielsweise:

- Server
- Router und Switches
- Virtuelle Systeme
- 3rd Party Netzwerkkameras

Dallmeier Produkte und über Dallmeier bezogene Fremdprodukte werden immer mit den zum Zeitpunkt des Versands aktuellen Updates und Sicherheits-Patches ausgeliefert.

Zum aktuellen Zeitpunkt werden entsprechende Updates und Patches bereits angeboten. Beachten Sie gegebenenfalls die aktuellen Informationen der relevanten Hersteller.

V1.0.0 2022-02-02