Security Advisory Log4Shell

Log4Shell (CVE-2021-44228) ist eine Zero-Day-Schwachstelle für die Ausführung von beliebigem Code im beliebten Java-Logging-Framework Log4j. Die Schwachstelle wurde am 24. November 2021 von Alibabas Cloud Security Team privat an Apache gemeldet und am 9. Dezember 2021 öffentlich bekannt gegeben. Die Schwachstelle macht sich zunutze, dass Log4j LDAP- und JNDI-Anfragen nicht prüft, so dass Angreifer beliebigen Java-Code auf einem Server oder einem anderen Computer ausführen können.

Beachten Sie zusätzlich zu diesem Advisory die zahlreichen Veröffentlichungen zu Log4Shell im Internet, wie beispielsweise eine (nicht abschließende) Veröffentlichung betroffener Dienste in einem github-Projekt. Beachten Sie auch entsprechende Meldungen des Bundesamt für Sicherheit in der Informationstechnik (BSI) oder des National Institute of Standard and Technology (NIST).

Keine Gefährdung

Dallmeier hat bereits alle Aufzeichnungssysteme, Kameras sowie Software-Produkte bezüglich der Log4Shell Schwachstelle überprüft. Das Framework **Log4j** wird in den folgenden Produkten **nicht eingesetzt**. Für diese Produkte besteht **keine Gefährdung** durch eine Ausnutzung der Log4Shell Schwachstelle.

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

Gefährdung

Die Experten von Dallmeier haben **eine Schwachstelle** in der Logging-Plattform der **HEMISPHERE® High Availability Lösung** festgestellt. Für die zugrunde liegende Open-Source-Software sind Patches und Updates verfügbar. Diese werden zeitnah in einem umfassenden **Infrastruktur-Update** zusammengefasst.

Maßnahmen

Die Experten von Dallmeier haben bereits eine **sofort verfügbare Lösung zur Behebung der Schwachstelle** in der HEMISPHERE® High Availability Lösung erarbeitet. Durch eine **Anpassung der Konfiguration** relevanter Systemkomponenten kann die **Ausnutzung der Log4Shell Schwachstelle verhindert** werden. Diese Anpassungen können remote im laufenden Betrieb vorgenommen werden.

Die HEMISPHERE® High Availability Lösung 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 die große Verbreitung** des Java-Logging-Framework Log4j eine Vielzahl von Geräten und Anwendungen für die Log4Shell 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 2021-12-14