01.01.2022 / cr

So sichern Sie den NetWorker gegen Angriffe über den Apache Log4j Code

Im Dezember hat dieses Problem in der gesamten IT-Welt eine Menge Staub aufgewirbelt. Es wurde bekannt, daß in der beliebten Java-Logging-Bibliothek Log4j eine Schwachstelle existiert. Über sie können relativ leicht Angriffe erfolgreich durchgeführt werden und großen Schaden in der IT-Infrastruktur anrichten. Und weil dies so kritisch ist, sind seit Mitte Dezember 2021 jede Menge Artikel über dieses Problem erschienen.

Zur Lösung des Problems hat Dell/EMC am 16.12.2021 eine neue Version seiner Java Engine, der sog. NRE Software (*NRE* steht für *NetWorker Runtime Environment*) freigegeben. Es handelt sich um die Version 8.0.11. Herunterladen können Sie die Software dort, wo Sie auch die NetWorker Software selbst finden:

https://www.dell.com/support/home/de-de/product-support/product/networker/drivers

Außerdem hat Dell/EMC das Dokument DSA-2021-280 veröffentlicht. Es trägt den Titel ...

DSA-2021-280: Dell EMC NetWorker Security Update for Apache Log4j Remote Code Execution Vulnerability (CVE-2021-44228)

... und enthält weitere Informationen und Workarounds.

Bitte beachten Sie:

- Es handelt sich ausschließlich um die NRE Software, die der NetWorker Server benötigt.
- NetWorker Storage Node, NetWorker Client, NetWorker Management Console, die NetWorker Management UI, NetWorker CloudBoost, and NetWorker vProxy sind nicht betroffen.
- Es handelt sich um einen Update für die NetWorker Versionen 19.3 und höher.
  Die älteren NetWorker Versionen 19.1.x und 19.2.x sind angeblich nicht betroffen.

Ich persönlich würde in jedem Fall die neueste NRE Version installieren.