Mit dem Dateiscan von Asset.Desk Name, Version und Ort von log4j-Dateien aufspüren

Für die „log4shell" oder auch „log4j" benannte Sicherheitslücke (CVE-2021-44228) wurde vom BSI die höchste Warnstufe Rot (IT-Bedrohungslage 4) bestimmt. Die Sicherheitslücke wird demnach als extrem kritisch eingestuft und gefährdet Ihre Dienste und Systeme im Regelbetrieb.

Betroffen sind die log4j-Bibliotheken von Version 2.0.1 bis 2.14.x. Ab der Version 2.15.0 ist das Problem gefixt. Versionen älter als 1.x sind nicht betroffen.

Mit dem Dateiscan des Asset.Desk Tracker sind Sie in der Lage, sämtliche log4j-Dateien auf den Windows Rechnern im Netzwerk aufzuspüren. Der Scanner ermittelt u.a. Rechnername, Dateiname, Version und Pfad. Damit setzt Sie Asset.Desk in die Lage festzustellen, wo überall log4j-Dateien residieren – und in welcher Version.

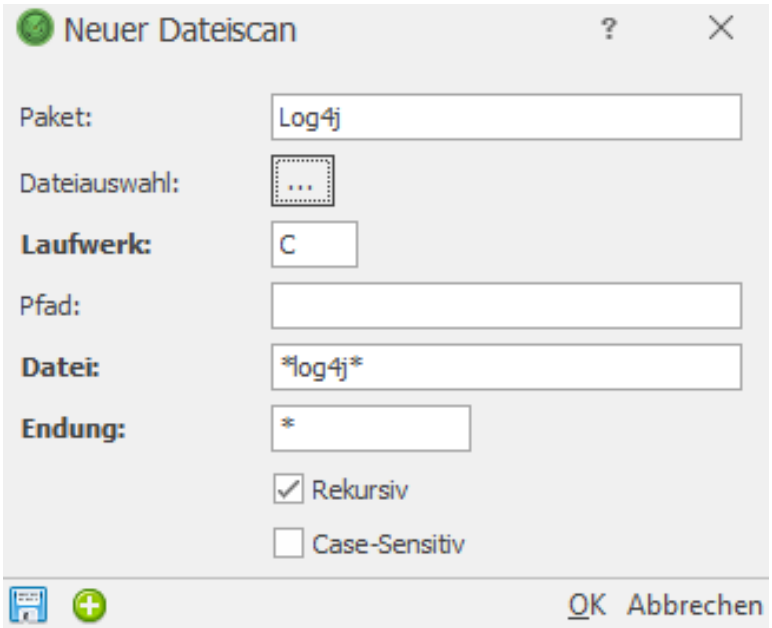
Sie erkennen anhand des Pfades die zugehörige Software-Anwendung, können prüfen, ob Sie bereits Kontakt zum Hersteller aufgenommen haben und, das ist besonders wichtig, ob für die log4j-Datei bereits der Fix (ab Version 2.15.0) installiert wurde.

Wie konfiguriere ich den Dateiscan für die log4j-Suche?

Starten Sie den **Asset.Desk Tracker** und gehen Sie in den Optionen zu **Windows Scan, Dateiscan.**

Drücken Sie auf der rechten Seite unterhalb der Liste „Neu". Erfassen Sie nun im Dateiscan-Dialog im Feld „Datei:" jeweils die Dateisuche für

- *log4j* - Hier sucht das System nach allen log4j-Dateien sämtlicher Versionen und/ oder
- *log4j*-2* - Hier sucht das System nach log4j-Dateien der Versionen 2.x

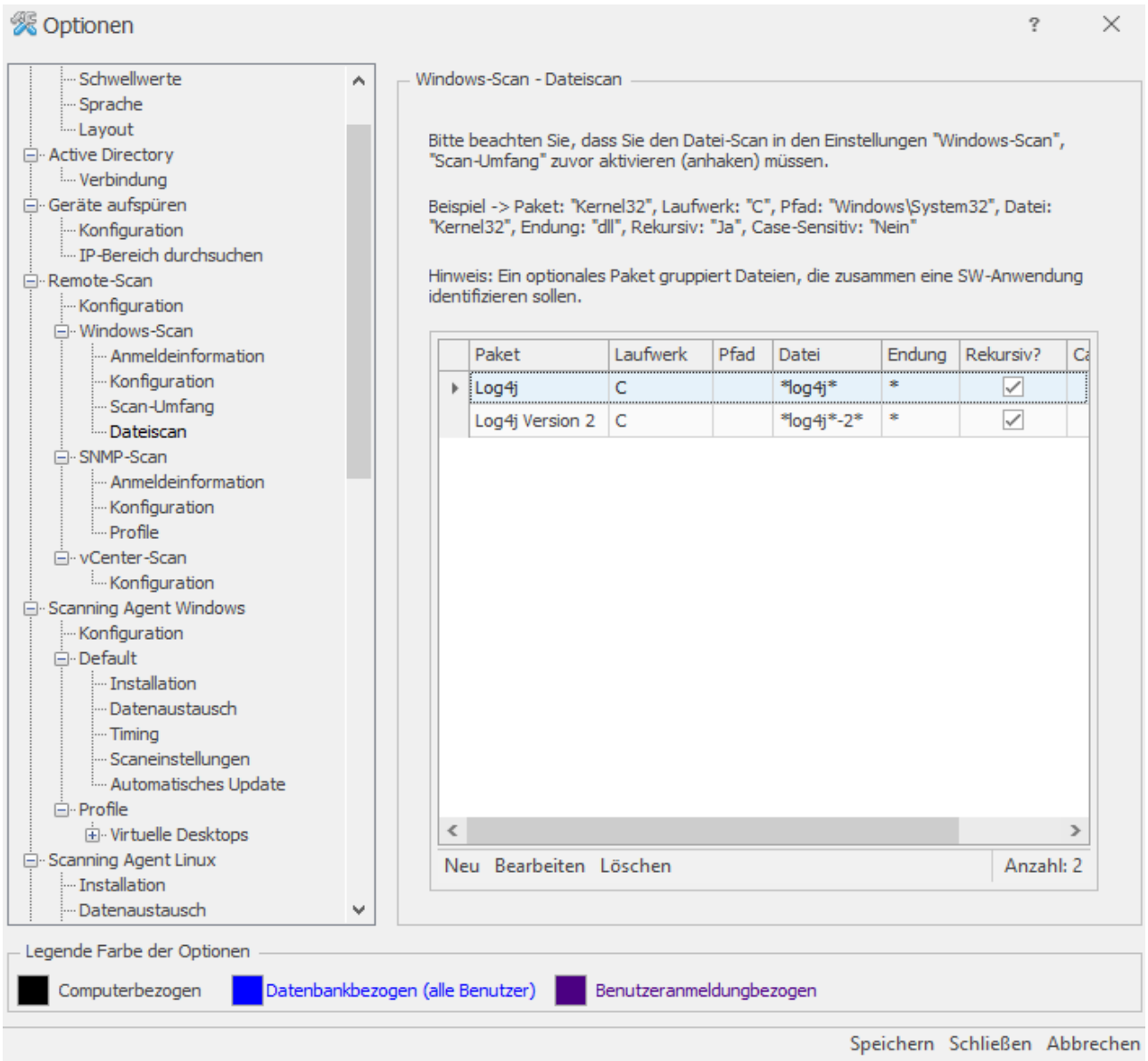


Sie können optional einen Paketnamen eintragen, z.B. „Log4j" bzw. „Log4j-2". In diesem Fall erscheinen die gefundenen log4j-Dateien am Gerät jeweils nur einmal unter diesem Produktnamen im Manager. Wenn Sie aber sämtliche log4j-Dateien am Zielgerät im Manager sehen wollen, dann lassen Sie den Paketnamen weg.

Als Laufwerk tragen Sie jeweils den Buchstaben des lokalen Laufwerks der Zielgeräte ein, in der Regel „C".

Wichtig ist der Haken bei „Rekursiv", damit auch alle Unterordner untersucht werden.

Nach Erfassung der Dateisuchen im Tracker sieht Ihre Dateiscan-Liste wie folgt aus:



Führen Sie anschließend den Scan der Zielgeräte nach Ihrem gewohnten Verfahren aus, entweder über den Remote-Scan im Tracker oder über den Scanning Agent Windows auf den Zielgeräten. Die Scan-Ergebnisse werden wie immer in den Manager übertragen.

Wie erhalte ich nun einen Überblick über die installierten log4j-Dateien und die betroffenen Geräte im Manager?

Öffnen Sie im Asset.Desk Manager den Bericht „Installierte Software" im Menü „Start", Gruppe „Berichte".

Hier können Sie nun filtern nach z.B. „log4j", um die betroffenen Rechner mit den log4j-Dateien aufzufinden. Tragen Sie im Feld „Software:" den String „Log4j" ein (Groß- und Kleinschreibung sind egal).

Drücken Sie nun rechts die „Suchen"-Schaltfläche. Anschließend werden die Rechner mit den log4j-Dateien gelistet. Bitte prüfen Sie vor allem die Versionen der angezeigten Dateien.

Ist die Version noch im Bereich von 2.0.1 bis 2.14.x, dann haben Sie ein Problem! Sie müssen anhand des Dateipfades nun die zugehörige Software-Anwendung auf dem Zielgerät ermitteln und den Softwarehersteller dieser Anwendung kontaktieren.

Viel Erfolg!