

Wichtige Sicherheitsinformation LOG4J (CVE-2021-44228)

Sehr geehrte Damen und Herren,

das Bundesamt für Sicherheit in der Informationstechnik hat eine Schwachstelle der höchsten Stufe (CVSS 10 - rot) gemeldet, welche eine Vielzahl von Systemen und Softwarelösungen betrifft.

Aktuell ist davon auszugehen, dass die meisten IT-Umgebungen davon betroffen sind.

Eine gefährliche Schwachstelle in der weit verbreiteten Software Log4J lässt die Alarmglocken des Bundesamtes für IT-Sicherheit läuten.

Log4J ist ein weitverbreiteter Softwarebaustein welcher massenhaft Einsatz findet, um Nutzerzugriffe zu protokollieren. Er ist daher oftmals tief in der Architektur von Software-Produkten verankert. Welche Produkte verwundbar sind und für welche es bereits Updates gibt, ist derzeit nicht vollständig überschaubar und daher im Einzelfall zu prüfen.

Es wird dringend empfohlen die gesamte IT auf entsprechende Schwachstellen zu prüfen und durch Updates und Änderungen der Sicherheitseinstellungen abzusichern.

Folgende Gefahren haben wir für Sie zusammengefasst:

Angreifer können auf Systemen mit ungestopfter Sicherheitslücke praktisch jeden beliebigen Programmcode (Schadcode) nachladen und ausführen. Was genau möglich ist, hängt vom jeweils angegriffenen System ab. Es könnte zum Beispiel sein, dass die Angreifer Daten abgreifen oder eine Hintertür aufmachen, die sie erst viel später verwenden. Etwa, um dann in das System einzudringen, wenn sich die Aufregung gelegt hat.

Man muss damit rechnen, dass Angreifer versuchen, möglichst viele Daten abzugreifen, etwa sensible Nutzerdaten, Zugangsdaten oder Zahlungsdaten. Denn mit solchen Daten lässt sich konkret Geld verdienen und Schaden anrichten. Aber auch für die weit verbreitete Bedrohung "Ransom Ware" eignet sich das Sicherheitsleck hervorragend: Es steht zu befürchten, dass in naher Zukunft mehr Erpressungsversuche über das Netz zu beobachten sind.

Doch auch Hardware könnte gefährdet sein. Insbesondere bei einigen öffentlichen WLAN-Systemen ist Log4J schon nachgewiesen. Auch Hardware am Homeoffice-Arbeitsplatz könnte gefährdet sein.

Als Ihr IT-Dienstleister möchten wir es nicht versäumen, Sie über diese Gefahren in Kenntnis zu setzen.

Bitte melden Sie sich bei unserer log4j - Support, damit wir die Bedrohungslage für Sie analysieren und beheben können.

Log4j-Support-Hotline: +49 541 3388488

Für Rückfragen stehen wir gerne zur Verfügung.

Mit freundlichen Grüßen

IT Sicherheitstechnik



DEK Telecom GmbH
Hakenbusch 1 | 49078 Osnabrück
Tel. +49 541 33884-0 | Fax +49 541 33884-111
support@dek.net | www.dek.net