WICHTIGE KUNDENINFORMATION

Stellungnahme zur LOG4 Shell Sicherheitslücke

Guten Tag,

kürzlich wurden Informationen zur Sicherheitslücke Log4Shell (CVE-2021-44228) veröffentlicht. Bereits nach wenigen Stunden wird diese aktiv für Angriffe aus dem Internet ausgenutzt. Der Schweregrad dieser Sicherheitslücke wird vom BSI mit dem größtmöglichen Schweregrad 10 eingestuft - daher wurde die IT-Bedrohungslage 4 - Rot ausgerufen.

Gleich vorweg: Die page one GmbH und die damit verbundenen Marken (scannerbox. printerbox.) sind von der Schwachstelle NICHT betroffen. Die Anwendungen scannerbox. Kanzlei & scannerbox. indexCREATOR basieren vollständig auf dem .NET-Framework, nicht auf Java. Die erwähnten Sicherheitslücken sind in dieser Bibliothek nicht enthalten.

DAS STECKT DAHINTER

Die Schwachstelle befindet sich in der Java-Codebibliothek „Log4j“, welche in verschiedensten Anwendungen enthalten sein kann. Hackern wird es hierdurch ermöglicht, durch Fernzugriff eigene Befehle auf den betroffenen Systemen auszuführen und diese zu kompromittieren. Einzig die Beseitigung dieser Schwachstelle in allen betroffenen Anwendungen durch entsprechende Maßnahmen schützt vor externen und ungewollten Zugriffen auf die eigenen Systeme.

INSBESONDERE ÖFFENTLICH ZUGÄNGLICHE SOFTWAREENDPUNKTE (INTERNETSEITEN, ETC.)

sind hiervon betroffen, nach Möglichkeit sollten jedoch auch interne Systeme schnellstmöglich aktualisiert werden. Wichtige Hinweise und Details sowie weiterführende Informationen vom BSI finden Sie **hier**.

SERVER SIND BEDROHT

Bei "log4j" handelt es sich um eine „beliebte Protokollierungsbibliothek für Java-Anwendungen. Sie dient der performanten Aggregation von Protokolldaten einer Anwendung“, wie es das BSI beschreibt. Die Lücke steckt also in einer Datei, die auf Servern zum Einsatz kommt und von Server-Administratoren entweder durch vorläufige Notmaßnahmen / Workarounds oder aber durch ein Update für log4j geschlossen werden muss. Endanwender können sich gegen diese Schwachstelle nicht schützen. Laut BSI sollten Produkte von über 140 Herstellern bedroht sein. Eine erste Liste mit betroffenen Unternehmen findet man hier.

WEITERE INFOS ZU UNSEREN VERTRIEBSPRODUKTEN:

Multifunktionsgerät (Drucker/Kopierer/Scanner) werden fast immer innerhalb Ihres Netzwerks betrieben und sind damit grundsätzlich durch Ihre eingesetzte Firewall deutlich weniger gefährdet.

Weitere Infos von Canon & NT-Ware erhalten Sie hier:

https://www.canon.de/support/product-security-latest-news/

https://www.uniflow.global/en/security/security-and-maintenance/

Die Anwendungen scannerbox. Kanzlei & scannerbox. indexCREATOR basieren vollständig auf dem .NET-Framework, nicht auf Java. Die erwähnten Sicherheitslücken sind in dieser Bibliothek nicht enthalten.

SCANNERBOX. MANDANT CONNECT & SCANNERBOX. MANDANT CONNECT II

setzen intern log4J ein. Dies ist allerdings für Hacker **nicht** durch externe Aufrufe **zugänglich**. Zudem ist auf dem verwendeten Betriebssystem Android kein JNDI-Paket enthalten, was Angriffe über die Lücke in Log4J unmöglich macht.

WEBSEITEN SCANNERBOX.DE UND PAGE-ONE.DE

Unsere Webseiten und Dienste wurden überprüft und sind **NICHT** von den Angriffen durch log4j betroffen. Unabhängig davon werden wir für unsere Produkte regelmäßig Softwareupdates zur Verfügung stellen.

Wir empfehlen allen unseren Kunden zu prüfen, ob log4j auf ihren eigenen Systemen eingesetzt wird und ggf. die entsprechenden Maßnahmen zu ergreifen.