Massive und gefährliche IT-Sicherheitslücke **Stand 13.12.2021**

Schempp Networks Factsheet Apache Log4j

Sehr geehrte Damen und Herren,
am Wochenende veröffentlichte das BSI (Bundesamt für Sicherheit in der Informationstechnik) ein Schreiben zu einer sehr bedrohlichen Sicherheitslücke in einer Open Source Software namens Log4j.
https://www.bsi.bund.de/SharedDocs/Cybersicherheitswarnungen/DE/2021/2021-549032-10F2.pdf?__blob=publicationFile&v=3
Die Sicherheitslücke hat einen Gefährdungswert: 10 von 10

Beschreibung
log4j ist ein Framework zum Loggen von Anwendungsmeldungen in Java. Innerhalb vieler Open-Source- und kommerzieller Softwareprodukte hat es sich über die Jahre zu einem De-facto-Standard entwickelt. log4j gilt als Vorreiter für andere Logging-Frameworks, auch in anderen Programmiersprachen.

Was bedeutet das im Klartext:
Aktuell versuchen Hacker aus aller Welt aus dem Internet erreichbare Systeme zu Scannen um die Schwachstelle aufzuspüren. Auch unsere Kunden und wir selbst werden von diesen Scans betroffen sein.
Die schlechte Nachricht:
Die oben genannte Technologie setzt so gut wie jeder große Softwarehersteller in irgendeinem seiner Produkte ein: VMWare, Cisco, Unifi, SAP, und und und.
Wird die Schwachstelle gefunden, kann sie genutzt werden, um uneingeschränkt Code auf dem Zielsystem auszuführen. Das bedeutet man kann mit dem System machen was auch immer man will. z.B. die komplette Kundendatenbank kopieren, Patente klauen oder Zugangsdaten ausspionieren z.B. zum Onlinebanking.

Die gute Nachricht:
Das Team der Schempp GmbH ist seit Sonntag damit beschäftigt die Sicherheitslücke zu analysieren.
Das allerwichtigste ist, dass Sie und Ihre Kollegen Ruhe bewahren.

Eines der größten Probleme der Sicherheitslücke ist, dass die Log4J Software (bzw. Framework) von so gut wie jedem Softwarehersteller eingesetzt wird. Das bedeutet, dass nicht nur die von uns verwaltete Basis der IT Betroffen ist, sondern vermutlich auch viele der Programme, die Sie im täglichen Gebrauch einsetzen.

Kunden die aktive Serviceverträge im Bereich Managed Firewall und Managed Endpoint Security oder IaaS mit uns haben werden Kunde für Kunde durchgegangen.

Dabei gehen wir wie folgt vor:
1. Analyse der Sicherheitsprotokolle aus Firewall und Endpoint Security
2. Bei Verdacht oder Fund von Vorkommnissen kontaktieren wir Sie proaktiv per Telefon
3. Wir besprechen telefonisch die nächsten Schritte

Diese drei Schritte wiederholen wir ab heute jeden Tag.

Bitte sehen Sie davon ab unsere Techniker zu dem Thema direkt telefonisch zu kontaktieren, wir benötigen alle Ressourcen für die Sicherheitsüberprüfungen.

So können Sie über Ihren Hersteller checken, ob Ihre Software Log4J einsetzt:
1. Öffnen Sie Google
2. Geben sie den unten genannten CVE Code + den Namen Ihrer Software ein z.B. CVE-2021-44228 SAP
3. Wenn der Hersteller schon Informationen zu der Lücke hat, werden Sie auf der Website etwas dazu finden.
4. Folgen Sie den Informationen und beauftragen Sie die Installation von Updates für Ihre Software
5. Sollten Sie keine Informationen finden, probieren Sie das gleiche am Folgetag
6. Haben Sie nach 7 Tagen keine Informationen gefunden, sollten Sie Ihren Systemhersteller per E-Mail kontaktieren und explizit nachfragen, ob das Log4J Framework in Ihrer Software zum Einsatz kommt.

Hier einige Dinge die Sie vielleicht checken sollten:
ERP System, CRM-System, Banking Software, Zeiterfassungssoftware, Buchhaltungs- Lohnabrechnungssoftware, Dokumentenmanagementsoftware, Telefonie Software, Videochatsoftware

Erklärungen:
CVE = Common Vulnerabilitys and Exposures = allgemeine Schwachstellen und Gefährdungen
Erklärung:
https://www.security-insider.de/was-ist-cve-a-771921/

Was können Sie als Kunde machen, um in der Zukunft noch sicherer zu sein:

1. Gemanagte Firewall von Schempp Networks einsetzen
2. Gemanagte Endpoint Security von Schempp Networks einsetzen
3. Permanente Securityaudits durchführen lassen

Wie immer gilt Ruhe bewahren und die Augen und Ohren offenhalten.

Liebe Grüße
Ihr Team von Schempp Networks