DEUTSCHE GESELLSCHAFT FÜR
CYBERSICHERHEIT

# Log4shell Schwachstelle mit cyberscan.io® erkennen

**Mit unserem Sicherheits-Tool cyberscan.io® können Sie Ihr System ab sofort auf die kritische Log4shell Sicherheitslücke überprüfen. Im Folgenden erklären wir Ihnen, wie cyberscan.io® dabei vorgeht.**

## 1

**Unsere regulären Scans von cyberscan.io®** nutzen aktuell mehrere Tests, um die Log4shell Schwachstelle in Systemen zu identifizieren. Diese Tests sind alle nach demselben Muster aufgebaut.

**cyberscan.io®** testet derzeit bei HTTP, SIP, TCP & UDP Verbindungen.
Dabei öffnet der Scanner bei sich einen zufälligen Port zwischen 0 & 65536 - je nach aktuellem Test unterschieden zwischen TCP & UDP.

Danach baut sich der Scanner als Payload den LDAP-STRING mit seiner eigenen externen IP und dem geöffneten Port als Callback Adresse.

Als Beispiel:
payload = *„${jndi:ldap://“ + ownip + „:“ + rnd_port + „/a}“;*

Anschließend „injected“ **cyberscan.io®** diesen String in verschiedene Anfragen, welche am wahrscheinlichsten auf Serverseite geloggt werden und wartet, ob sich das Ziel auf dem geöffneten Port zurückmeldet.

- Bei HTTP Anfragen verwendet **cyberscan.io®** die URL, den „Referer“ sowie den „User-Agent“ um den Payload einzuschleusen.

- Bei SIP Anfragen verwenden wir den „User-Agent“ sowie das „Contact“ Feld.

Zuletzt wartet der Scanner jeweils 5 Sekunden auf eine Anfrage auf dem zuvor geöffneten Port. Kommt innerhalb der Zeit eine Antwort, sehen wir das als Treffer an und Ihr System ist höchstwahrscheinlich von der Log4shell Schwachstelle betroffen. **Ein Nachladen von weiterem Code findet nicht statt!**

Zu erwähnen ist noch, dass die vier verschiedenen Protokolle (HTTP, SIP, TCP & UDP) jeweils auf unterschiedlichen Ports lauschen, sodass eine Zuordnung möglich ist und entsprechend dargestellt werden kann. Auf diese Weise erhalten Sie Anhaltspunkte, welcher Dienst betroffen ist.

## 2

Zusätzlich zu den regulären Rescans über **cyberscan.io®**, werden wir über das Tool in den kommenden Tagen all unsere Kunden automatisiert scannen, um zu überprüfen, ob diese von der Log4shell Sicherheitslücke betroffen sind. Hier werden gezielt sämtliche extern erreichbaren IP-Adressen des Kunden überprüft.

Dieser automatisierte Scan arbeitet mit eigenen DNS & LDAP Servern sowie Tokens zur Zuordnung. Anfang der Woche haben wir ein erstes Skript zur Verfügung gestellt, welches als Callback den canarytoken.com Service nutzte. Mittlerweile verwenden wir hier jedoch komplett eigene Dienste.

Der Massenscan wird deutlich mehr Header, Cookies und häufig verwendete POST Parameter nutzen und zudem versuchen, an den Filtern einer Web Application Firewall (WAF) vorbeizukommen.

Wenn Sie darüber hinaus noch Hilfe benötigen, stehen wir Ihnen jederzeit gerne zur Verfügung.

**Bleiben Sie sicher!**
**Ihr DGC Team**

Deutsche Gesellschaft für Cybersicherheit mbH & Co.KG
Geschäftsführer: Matthias Nehls
Am Fördeufer 1b
DE-24939 Flensburg

T +49.461.995 838 0
F +49.461.995 838 99

info@dgc.org
www.dgc.org