# Aktuelle SophosLabs-Erkenntnisse zur Apache-Log4Shell-Schwachstelle:

- Sophos verzeichnet eine rasche Zunahme von Angriffen, die die Sicherheitslücke ausnutzen oder versuchen, diese auszunutzen. Bisher wurden Hunderttausende von Versuchen erkannt
- Cryptomining-Botnetze gehören momentan zu den häufigsten Angriffsformen. Dabei konzentrieren sich die Botnetze auf Linux-Serverplattformen, die der Schwachstelle besonders ausgesetzt sind
- Sophos hat auch Versuche gesehen, Informationen aus Diensten zu extrahieren, einschließlich Amazon-Web-Services-Schlüsseln und anderen privaten Daten
- Sophos hat festgestellt, dass Versuche, Netzwerkdienste auszunutzen, mit der Suche nach verschiedenen Service-Typen beginnen. Etwa 90 Prozent der von Sophos erkannten „Testläufe“ konzentrierten sich auf das Lightweight Directory Access Protocol (LDAP). Eine kleinere Anzahl zielte auf Javas Remote Interface (RMI) ab, wobei es in diesem Bereich anscheinend eine größere Vielfalt einzigartiger, RMI-bezogener Versuche gibt.
- Sophos erwartet, dass Angreifer in den kommenden Tagen und Wochen ihre Angriffsmethoden intensivieren und diversifizieren, einschließlich der Möglichkeit, Ransomware zu nutzen

Sean Gallagher, Senior Threat Researcher bei Sophos, über die aktuelle Lage:
„Seit dem 9. Dezember hat Sophos Hunderttausende von Versuchen erkannt, Code mithilfe der Sicherheitslücke Log4Shell aus der Ferne auszuführen. Dabei handelte es sich zunächst um Proof-of-Concept (PoC) Exploit-Tests, sowohl von Sicherheitsforschers als auch potenziellen Angreifern, sowie viele Online-Scans in Bezug auf die Schwachstelle. Allerdings folgten schnell Versuche, sogenannte Coin-Miner zu installieren, darunter das Kinsing-Miner-Botnetz und auch die von Amazon-Web-Service-Konten verwendeten Schlüssel stehen im Fokus. Zudem gibt es vermehrt Anzeichen dafür, dass Angreifer versuchen, die Schwachstelle auszunutzen, um Remotezugriffstools wie Cobalt Strike in Opfernetzwerken zu installieren, um potenzielle Ransomware-Angriffe vorzubereiten.“

„Log4Shell stellt Verteidiger vor eine besondere Herausforderung. Viele Softwareschwachstellen sind auf ein bestimmtes Produkt oder eine bestimmte Plattform beschränkt, wie beispielsweise die ProxyLogon- oder ProxyShell-Schwachstellen in Microsoft Exchange. Sobald die Verteidiger wissen, welche Software anfällig ist, können sie sie überprüfen und patchen. Log4Shell ist jedoch eine Bibliothek, die von vielen Produkten verwendet wird. Es kann daher in den dunkelsten Ecken der Infrastruktur einer Organisation präsent sein, zum Beispiel in jeder selbst entwickelten Software. Das Auffinden aller Systeme, die aufgrund von Log4Shell anfällig sind, sollte eine Priorität für die IT-Sicherheit sein.“

„Sophos geht davon aus, dass sich die Geschwindigkeit, mit der sich Angreifer die Schwachstelle zunutze machen, in den kommenden Tagen und Wochen weiter intensiviert und diversifiziert. Hat sich ein Angreifer erst einmal den Zugang zu einem Netzwerk gesichert, ist leider fast alles möglich. Daher müssen IT-Sicherheitsteams, neben dem bereits von Apache in Log4j 2.15.0 veröffentlichten Software-Update eine gründliche Überprüfung der Aktivitäten im Netzwerk durchführen, um alle Spuren von Eindringlingen zu erkennen und zu entfernen, selbst wenn es nur nach lästiger Commodity-Malware aussieht.“

Auch Paul Ducklin, IT-Security-Experte bei Sophos, betont die Wichtigkeit für IT-Teams, dieses Problem sehr ernst zu nehmen:
„Technologien wie IPS, WAF und intelligente Netzwerkfilterung tragen dazu bei, diese globale Schwachstelle unter Kontrolle zu bringen. Aber die unglaubliche Anzahl verschiedener Möglichkeiten, wie der Log4Shell-Triggertext kodiert werden kann, die große Anzahl verschiedener Stellen im Netzwerkverkehr, an denen diese Zeichenfolgen auftreten können, und die große Vielfalt an Servern und Diensten, die betroffen sein könnten, machen Log4Shell zu einer ganz besonderen Herausforderung für Sicherheitsexperten."

**Neu: Social Media von Sophos für die Presse**
Wir haben speziell für Sie als Journalist*in unsere Social-Media-Kanäle angepasst und aufgebaut. Hier tauschen wir uns gerne mit Ihnen aus. Wir bieten Ihnen Statements, Beiträge und Meinungen zu aktuellen Themen und natürlich den direkten Kontakt zu den Sophos Security-Spezialisten.
Folgen Sie uns auf und

LinkedIn: http://www.linkedin.com/groups/9054356/
Twitter: @sophos_info

**Pressekontakt:**

Sophos
Jörg Schindler, PR-Manager Central & Eastern Europe
joerg.schindler@sophos.com, +49-721-25516-263

TC Communications
Arno Lücht, +49-8081-954619
Thilo Christ, +49-8081-954617
Ulrike Masztalerz, +49-30-55248198
Ariane Wendt +49-172-4536839
sophos@tc-communications.de