Noch blieb das große Log4Shell-Beben aus – ein forensischer Status-Befund

„Auch wenn die befürchtete, massenhafte Ausnutzung der Log4Shell-Schwachstelle bisher noch nicht stattgefunden hat, wird der Bug noch jahrelang ein Ziel für Angriffe sein“, Chester Wisniewski, Principal Research Scientist bei Sophos.

Die Experten-Teams von Sophos haben die Ereignisse rund um die Log4Shell-Schwachstelle seit der Entdeckung im Dezember 2021 forensisch analysiert und eine erste Bilanz gezogen – inklusive einer Zukunftsprognose von Principal Research Scientist Chester Wisniewski sowie verschiedenen Grafiken, die die Ausnutzung der Schwachstelle zeigen. Das Resümee: Die große Krise aufgrund massenhafter Ausnutzung durch Cyberkriminelle blieb bisher aus, obwohl eine solche branchenweit befürchtet wurde. Allerdings bedeutet das Ausbleiben der erwarteten und verheerenden Auswirkungen keine Entwarnung. Denn der Log4Shell-Bug, der tief in vielen digitalen Anwendungen und Produkten verborgen ist, kann voraussichtlich noch jahrelang ein Ziel der Cyberkriminellen sein.

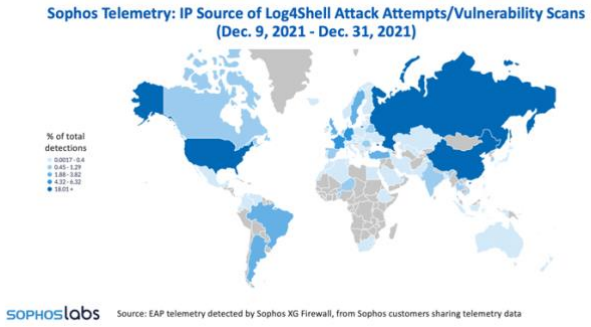
Die Sophos-Expert:innen sind der Meinung, dass die unmittelbaren und massenhaften Angriffe auf die Log4Shell-Lücke vor allem durch aktives Handeln aller Beteiligten bisher erfolgreich eingedämmt werden konnten. Die Tragweite der Schwachstelle hat die Digital- und Sicherheits-Community erfolgreich vereint. Ein gemeinschaftliches Vorgehen ist nicht neu, bereits im Jahr 2000 beim Y2K-Bug war dies der Fall, und es scheint auch hier einen großen Unterschied gemacht zu haben. Im Augenblick, als die Details der Log4j-Sicherheitslücke bekannt wurden, haben die weltweit größten und wichtigsten Cloud-Dienste, Softwareanbieter und Unternehmen Maßnahmen ergriffen, um sich von dem Eisberg fernzuhalten und eine Katastrophe zu verhindern. Möglich war dies auch durch die gemeinschaftliche Intelligenz und praktischen Anleitungen der Security-Gemeinschaft.

Begrenzte Massenausbreitung

Das Sophos Managed Threat Response Team (MTR) stellte fest, dass zwar viele Scans und Versuche, den Log4Shell-Exploit auszunutzen, entdeckt wurden, jedoch bis Anfang Januar 2022 nur wenige MTR-Kunden konkret mit Einbruchsversuchen via Log4j konfrontiert waren. Eine Erklärung dafür könnte die Notwendigkeit sein, dass der Angriff an jede Anwendung, die den anfälligen Apache Log4J-Code enthält, angepasst werden muss.
Daher werden die weit verbreiteten Anwendungen, die die Schwachstelle enthalten, in größerem Umfang auf automatisierte Weise ausgenutzt als andere. Ein Beispiel dafür ist VMware Horizon – hier fand der erste von Sophos MTR beobachtete Einbruch über die Log4Shell-Lücke statt.

Deutliche Verschiebungen in der Geo-Telemetrie

Die Sophos-Geo-Telemetrie seit der Entdeckung der Schwachstelle bis in die ersten beiden Januarwochen 2022 zeigt interessante Variationen bei den Quellen der Angriffsversuche und Scans. Die Karte im Dezember 2021 macht deutlich, dass Regionen wie die USA, Russland, China, Westeuropa und Lateinamerika stärker betroffen sind. Die starke Gewichtung der USA und Deutschlands in den geografischen IP-Quelldaten spiegelt wahrscheinlich die großen Rechenzentren wider, die dort angesiedelt sind, wie beispielsweise von Amazon, Microsoft und Google.



Dieses Lagebild und die Anzahl der erkannten Vorfälle ändern sich Anfang 2022 dramatisch. Der auffälligste Unterschied ist, dass die anfängliche Dominanz Russlands und Chinas im Januar abgenommen zu haben scheint. Nach Erkenntnissen von Sophos spiegelt dies einen offensichtlichen Rückgang der Angriffsversuche durch eine kleine Anzahl hochaggressiver Kryptoanalysten in diesen Regionen wider.

Fazit:
Die Experten-Teams von Sophos sind der Ansicht, dass Versuche, die Log4Shell-Schwachstelle auszunutzen, wahrscheinlich noch jahrelang andauern werden und ein beliebtes Ziel für Penetrationstester und für Nationalstaaten sowie deren Bedrohungsakteuren sein werden. Die Dringlichkeit, herauszufinden, wo die Schwachstelle eventuell im eigenen Netzwerk auftritt, und das Patchen entsprechender Anwendungen bleibt deshalb wichtigstes Ziel.

Der komplette englische Bericht mit weiteren Ergebnissen und grafischen Darstellungen steht hier zum Download bereit.

Zusätzliche Informationsquellen zu Log4Shell
Zudem hat Sophos seit der Entdeckung eine Reihe von weiteren Artikeln zu Log4Shell und zur Reaktion auf die Bedrohung veröffentlicht:

- Log4Shell Hell – Anatomy of an Exploit Outbreak
- Inside the Code – How the Log4Shell Exploit Works
- Log4Shell – Response and Mitigation Recommendations
- Log4jam – Log4J Exploit Attempts Continue in Globally Distributed Scams, Attacks

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