Log4Shell Reloaded: Angreifer nutzen die Schwachstelle für dauerhaften Server-Zugang

Forscher der SophosLabs entdeckten drei Hintertüren und vier Cryptominer, die auf ungepatchte VMware Horizon Server zielen, um dauerhaft Zugang zu erlangen

Wiesbaden, 29. März 2022 – Sophos veröffentlicht heute seine jüngsten Forschungsergebnisse zur Log4Shell-Schwachstelle. Angreifer nutzen diese, um Hintertüren einzubauen und Skripte für ungepatchte VMware Horizon Server zu erstellen. Dadurch erhalten sie dauerhaften Zugang auf VMware Horizon Server für zukünftige Ransomware-Attacken. In dem detaillierten Bericht Horde of Miner Bots and Backdoors Leveraged Log4J to Attack VMware Horizon Servers beschreiben die Sophos-Forscher die Werkzeuge und Techniken für die Kompromittierung von Servern sowie drei unterschiedliche Hintertüren und vier Cryptominer. Die Hintertüren kommen möglicherweise von Access Brokern.

Log4Shell ist eine Schwachstelle in der Java-Codebibliothek Log4J. Wenn Angreifer diese Lücke ausnutzen, erhalten sie die Möglichkeit, jeden System-Code ihrer Wahl auszuführen. Sie ist eingebettet in Hunderte von Software-Produkten und Ende 2021 bekannt geworden. Die jüngsten Angriffsmöglichkeiten, die Log4Shell einsetzen, um anfällige Horizon Server anzugreifen, beinhalten:

- zwei legitime Monitoring und Management-Werkzeuge für den Fernzugriff – Atera Agent und Splashtop Streamer
- die bösartige Sliver-Hintertür
- die Cryptominer z0Miner, JavaX miner, Jin und Mimu
- verschiedene auf Power-Shell basierende Reverse Shells, die Geräte und Backup-Informationen sammeln

Die Sophos-Analyse zeigt, dass Sliver manchmal zusammen mit Atera- und PowerShell-Profiling-Skripten geliefert und zur Übermittlung von Jin- und Mimu-Varianten der XMrig Monero Schürfer-Botnets genutzt wird. Die Angreifer verwenden unterschiedliche Vorgehensweisen, um ihre Ziele zu infizieren. Während einige der früheren Attacken Cobalt Strike zum Bereitstellen und Ausführen der Cryptominer einsetzen, begann die größte Welle der Angriffe Mitte Januar 2022: Sie führte das Cryptominer-Installations-Skript direkt von der Apache-Tomcat-Komponente des VMware Horizon Servers aus. Diese Welle der Angriffe ist immer noch aktiv.

„Weit verbreitete Anwendungen wie VMware Horizon, die manuell aktualisiert werden müssen, sind besonders anfällig für Ausnutzungen im großen Stil“, so Sean Gallagher, Senior Security Researcher bei Sophos. „Unsere Untersuchung zeigen seit Januar 2022 Angriffswellen auf Horizon-Server, die verschiedene Hintertüren und Cryptominer für ungepatchte Server mitbringen, plus Skripte, um Geräteinformationen zu sammeln. Wir sind der Ansicht, dass einige der Hintertüren von Access Brokern geliefert sein könnten, die nach einem dauerhafte Remote-Zugang suchten und diesen wiederum anderen Angreifern verkaufen können, ähnlich wie Ransomware-Betreiber.“

Was Unternehmen jetzt tun sollten:
Die Sophos-Analyse gibt Hinweise drauf, dass mehrerer Kontrahenten diese Angriffe ausführen. Der wichtigste präventive Schritt wäre demnach, alle Geräte und Anwendungen mit der gepatchten Version der Software zu aktualisieren, die Log4J enthalten, inklusive der gepatchten VMware Horizon, sofern Organisationen die Applikationen in ihren Netzwerken verwenden. Log4J ist in Hunderten von Software-Produkte installiert, und vielen Unternehmen ist die Schwachstelle, die innerhalb ihrer Infrastruktur lauert, gar nicht bewusst, besonders bei gewerblicher, Open-Source- oder individueller Software, die keine reguläre Sicherheitsbetreuung hat. Selbst gepatchte Programme bieten keinen Schutz, wenn Angreifer bereits in der Lage waren, eine Web Shell oder eine Hintertür im Netzwerk zu installieren. Verteidigung in der Tiefe plus sofortigem Handeln bei jeglichem Hinweis auf z.B. Schürfer und andere ungewöhnliche Aktivitäten ist entscheidend, um derartigen Attacken nicht zum Opfer zu fallen.

Sophos hat weiterhin Angriffsaktivitäten in Verbindung mit der Log4Shell Schwachstelle genau beobachtet und eine Reihe technisch detaillierter und ratgebender Berichte veröffentlicht:

Log4Shell Hell – Anatomy of an Exploit Outbreak,

Log4Shell Response and Mitigation Recommendations,

Inside the Code: How the Log4Shell Exploit Works,

Log4Shell: No Mass Abuse, But No Respite, What Happened?

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: https://www.linkedin.com/groups/9054356/
Twitter: @sophos_info

Über Sophos
Sophos ist ein weltweit führender Anbieter von Next Generation Cybersecurity und schützt mehr als 500.000 Unternehmen und Millionen von Verbrauchern in mehr als 150 Ländern vor den modernsten Cyberbedrohungen. Basierend auf Threat Intelligence, KI und maschinellem Lernen aus den SophosLabs und von SophosAI bietet Sophos ein breites Portfolio an fortschrittlichen Produkten und Services, um Anwender, Netzwerke und Endpoints vor Ransomware, Malware, Exploits, Phishing und einer Vielzahl anderer Cyberattacken zu schützen. Sophos bietet mit Sophos Central eine einzige, integrierte und cloudbasierte Management-Konsole. Sie ist das Herzstück eines anpassungsfähigen Cybersecurity-Ökosystems mit einem zentralen Data Lake, der eine Vielzahl offener API-Schnittstellen bedient, die Kunden, Partnern, Entwicklern und anderen Cybersecurity-Anbietern zur Verfügung stehen. Sophos vertreibt seine Produkte und Services über Partner und Managed Service Provider (MSPs) weltweit. Der Sophos-Hauptsitz ist in Oxford, U.K. Weitere Informationen unter http://www.sophos.de.

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