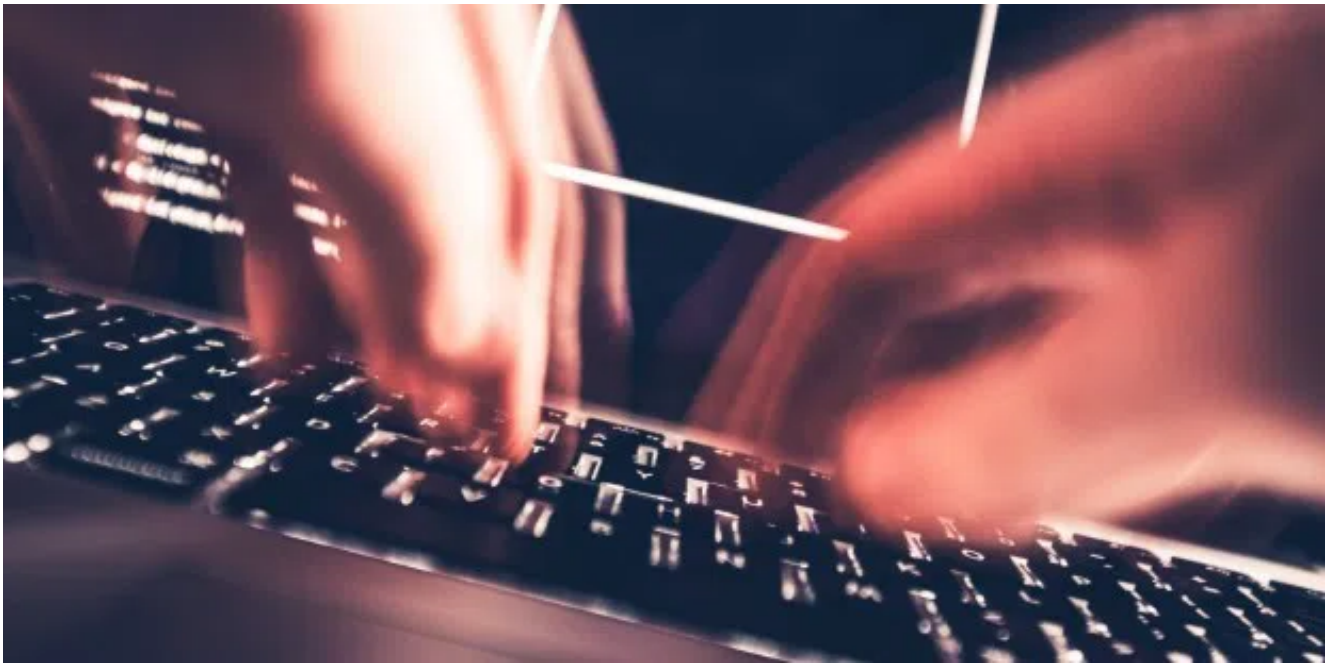
Log4Shell: Riesen-Sicherheitslücke log4j in vielen bekannten Systemen - aktueller Stand

Hans-Christian Dirscherl

In Minecraft und Steam, aber auch in vielen anderen Systemen steckt eine ernste Sicherheitslücke. Angreifer können damit ihren Code auf fremden Systemen ausführen. Das BSI vergab die höchste Warnstufe für diese bereits ausgenutzte Zero-Day-Lücke. Update: Kaspersky und Apple.



Vergrößern **log4j: Riesen-Sicherheitslücke in Minecraft, iCloud, Steam etc.**

Update 14.12.: Das russische IT-Sicherheitsunternehmen Kaspersky hat mitgeteilt, dass seine Sicherheits-Produkte Log4Shell-Angriffe erkennen und blockieren, und zwar unter folgender Kennung:

Kaspersky rät zu diesen Maßnahmen, um sich gegen Log4Shell/log4j zu schützen:

Auch iCloud war von der log4j-Lücke betroffen, Apple scheint aber diese Schwachstelle bereits geschlossen zu haben.

Update Ende

Das Bundesamt für Sicherheit in der Informationstechnologie BSI hat die Gefährlichkeit einer am Freitag bekannt gewordenen Sicherheitslücke auf „Rot“ hochgestuft . Das ist die höchste Warnstufe!

Die kritische Schwachstelle entdeckten Sicherheitsexperten in "log4j" und zwar in dessen Versionen 2.0 bis 2.14.1. Auch alte 1er-Versionen von log4j scheinen wohl anfällig zu sein.

Server sind bedroht

Bei "log4j" handelt es sich um eine „beliebte Protokollierungsbibliothek für Java-Anwendungen. Sie dient der performanten Aggregation von Protokolldaten einer Anwendung“, wie es das BSI beschreibt. Die Lücke steckt also in einer Datei, die auf Servern zum Einsatz

kommt und von Server-Administratoren entweder durch vorläufige Notmaßnahmen / Workarounds oder aber durch ein Update für log4j geschlossen werden muss. Endanwender können sich gegen diese Schwachstelle nicht schützen. Laut BSI sollten Produkte von über 140 Herstellern bedroht sein. Eine erste Liste mit betroffenen Unternehmen findet man hier.

Das Sicherheits-Unternehmen Sophos beschreibt die Lücke folgendermaßen: 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."

Die, wie gesagt, auch als „Log4Shell" bezeichnete Lücke können Angreifer ausnutzen, um auf dem angegriffenen System ihren eigenen Programmcode auszuführen. Die Angreifer müssen hierzu nur bestimmte Zeichenketten an den Server schicken und diese Zeichenketten müssen von log4j verarbeitet werden. Beim iPhone funktioniert(e) dieser Angriff, indem man den Namen des iPhones durch eine entsprechende Zeichenfolge ersetzt und damit eine Anfrage an die iCloud-Server schickt.

Apple scheint diese Lücke aber mittlerweile geschlossen zu haben. Bei Minecraft erfolgt der Angriff wiederum dadurch, dass man im Chat die entsprechende

Zeichenfolge eintippt, wie Spiegel Online berichtet . Danach kann der Angreifer den entsprechenden Minecraft-Server kapern.

Laut BSI scannen Hacker bereits Server auf deren Anfälligkeit für diese Schwachstelle. In einigen Fällen konnten Angreifer die Lücke bereits erfolgreich ausnutzen, unter anderem mit Kryptominern, wie auch Bleeping Computer berichtet . Die derart kompromittierten Server schürfen dann also Kryptowährungen. Außerdem sollen bereits Botnetze diese Lücke ausnutzen.

Wie sind Endanwender betroffen?

Sophos beschreibt die Folgen/Gefahren für Endanwender so: "Log4Shell bedeutet nicht nur Alarmstufe Rot für Unternehmen, sondern auch private Nutzer können von den Auswirkungen der Lücke betroffen sein. Das gilt vorwiegend 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."

Einige Unternehmen/Einrichtungen wie VMware, Apache oder Unifi haben bereits Patches veröffentlicht. Diese sollten Administratoren schnellstmöglich aufspielen. Für log4j gilt die Version 2.15.0 als sicher, diese sollten Administratoren also zeitnah installieren. Bis durch Updates die Lücke geschlossen ist, sollten Administratoren Sicherheitsmaßnahmen ergreifen, die das BSI hier beschreibt . Das besondere elektronische Anwaltspostfach (BeA) wurde wegen dieser Lücke bereits abgeschaltet.