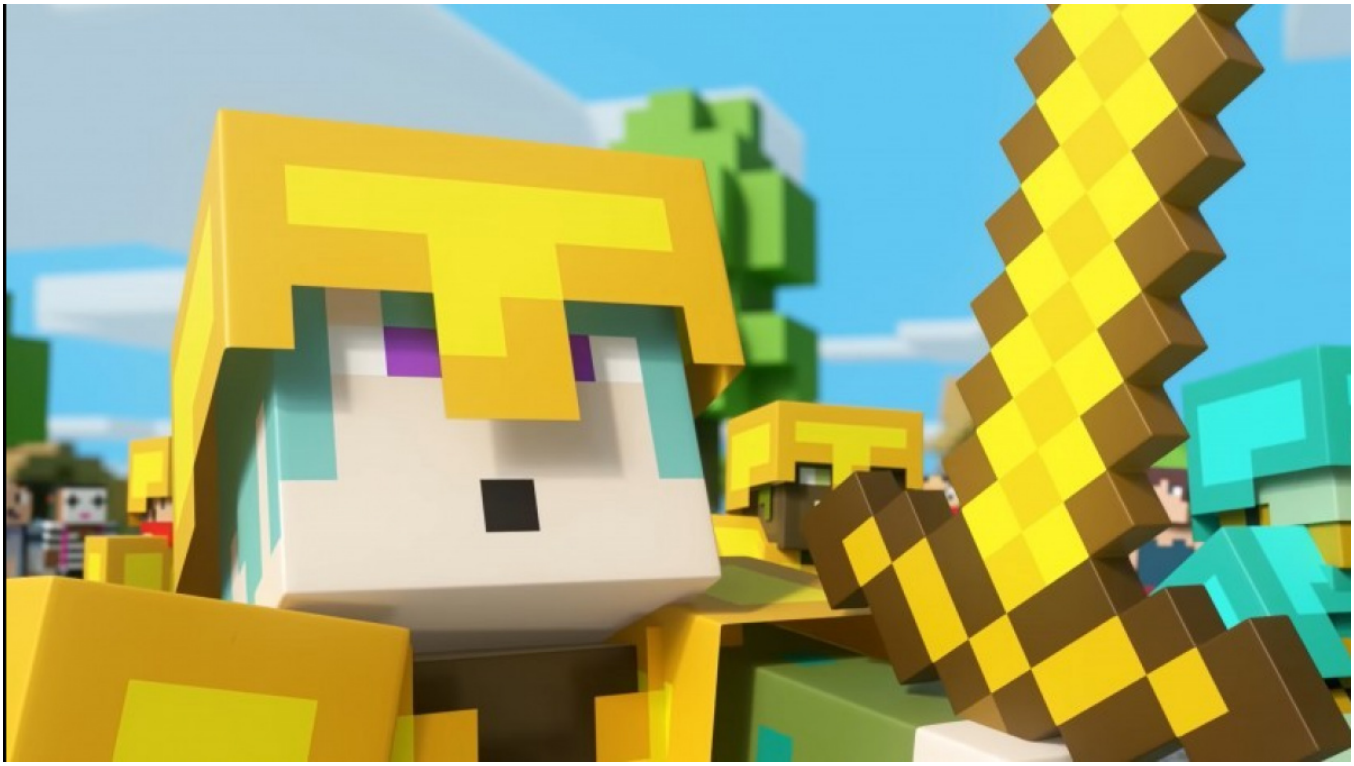
JAVA: Log4J-Lücke bedroht Minecraft und viele weitere Anwendungen

Das weit verbreitete Logging-Werkzeug Log4J lässt sich unter Umständen sehr leicht übernehmen. Betroffen ist auch Minecraft.

Sebastian Grüner 10. Dezember 2021, 13:05 Uhr



Die Java-Version von Minecraft ist von einer Sicherheitslücke betroffen, wie eventuell viele andere Anwendungen auch. (Bild: Microsoft)

Ein vermutlich aus China stammender Hacker hat Code zum Ausnutzen einer Sicherheitslücke in dem Logging-Werkzeug Log4J veröffentlicht. Das Brisante daran ist vor allem, dass sich die Lücke unter bestimmten Umständen wohl sehr leicht ausnutzen lässt und das Open-Source-Werkzeug Log4J zusätzlich dazu sehr weit verbreitet ist und in zahlreichen Web-Anwendungen zum Einsatz kommt.

Wie Arstechnica berichtet, sind zuerst Seiten auf die Lücke aufmerksam

geworden, die sich an die Spieler von Minecraft richten. Dort ist davor gewarnt worden, dass die Client- und Server-Versionen von Minecraft auf Basis von Java von der Lücke betroffen seien und zum Ausnutzen der Lücke auch Chat-Nachrichten ausreichen könnten. Theoretisch ließen sich so sämtliche Clients übernehmen, die sich an einem bestimmten Minecraft-Server anmelden.

Der Entwickler Mikael Hedberg alias Slicedlime bestätigt auf Twitter die gravierende Lücke und empfiehlt allen Nutzern einen Neustart. Der Launcher lädt dabei ein Update herunter, das die Lücke schließt. Server-Hosts sollten eine Konfiguration ändern, ein Update für den Minecraft-Server soll folgen.

Wenig Voraussetzungen für erfolgreiches Ausnutzen

Zur Lücke selbst schreiben die Sicherheitsspezialisten von Luna Sec, dass neben der verwundbaren Log4J-Version nur zwei Bedingungen für ein erfolgreiches Ausnutzen der Lücke notwendig seien. Zum einen braucht es dafür irgendeine Art Endpunkt, der per Protokoll-Aufruf (HTTP, TCP u.a.) verfügbar ist und Strings entgegennimmt. Hinzukommen muss dann nur noch ein Log-Aufruf, der jenen String über Log4J loggt.

In dem zuerst veröffentlichten Exploit wird durch den Aufruf dann via JNDI und LDAP auf eine Server-Instanz mit weiterem Schadcode verwiesen. Dabei wird aber nicht überprüft, ob es sich bei dem aufgerufenen Server um einen unter eigener Kontrolle handelt oder nicht. Das ermöglicht letztlich die Angriffe von außen.

Laut Luna Sec sind zwar einige Java-Versionen von dem Vorgehen über LDAP wegen anderer Vorkehrungen nicht konkret betroffen, es gebe für die Sicherheitslücke aber auch noch andere Angriffsvektoren, heißt es. Ähnliche Angriffe über JNDI werden seit Jahren immer wieder beschrieben.

Wie erwähnt ist Log4J extrem weit verbreitet und wird in vielen Projekten der Apache Foundation verwendet, wie etwa Flink, Solr oder Struts2. Auf

dem Portal Hackernews wird außerdem berichtet, dass unter anderem auch Valves Steam oder Apples iCloud anfällig für die Lücke seien. Das gesamte Ausmaß der eventuell betroffenen Anwendungen und Online-Dienste ist derzeit noch nicht absehbar.

Auf Twitter gibt es inzwischen aber auch kleine und kurze Beispiele, die zeigen, wie die Lücke in Desktop-Anwendungen wie Ghidra ausgenutzt werden kann, wenn dort Dateien geladen werden. Es ist also davon auszugehen, dass eigentlich alle Anwendungen, die die Funktionen von Log4J samt JNDI für eigene Zwecke verwenden, verwundbar sein könnten.

Die Sicherheitslücke wird inzwischen mit der CVE-Nummer CVE-2021-44228 bezeichnet. Laut dem dazugehörigen Security-Eintrag der Entwickler sei das verwundbare Verhalten ab Version 2.15 deaktiviert. Diese steht zum Download bereit. Die Versionen 2.0 bis 2.14.1 seien jedoch theoretisch verwundbar. Gefunden worden ist die Lücke laut der Apache Foundation von Chen Zhaojun von Alibabas Cloud Security Team.