Archiv

Kritische Sicherheitslücke Log4Shell

Software-Fehler macht viele Server und Apps angreifbar

Es passiert nicht oft, dass das Bundesamt für Sicherheit in der Informationstechnik (BSI) eine Schwachstelle mit ihrer höchsten Warnstufe Rot versieht. So eine Sicherheitslücke – Log4Shell – hat sich gerade aufgetan. Sie öffnet Hackern Tür und Tor für Angriffe auf zahlreiche Server, Firmennetzwerke und Apps.

Von Peter Welchering | 13.12.2021

Hören 04:49 Audio herunterladen

Die Sicherheitslücke Log4Shell erlaubt es Angreifern, verwundbare Server mithilfe manipulierter Anfragen zu kapern. (picture alliance/dpa | Sebastian Gollnow)

Was macht diese Sicherheitslücke so gefährlich?

Bei der Sicherheitslücke Log4Shell geht es um fehlerhaften Code aus einer Java-Bibliothek namens Log4j. Viele kommerzielle Softwarepakete nutzen diese Bibliothek, um zu protokollieren, wer mit dieser Software arbeitet und wer auf welche Server zugreift. Brisant ist das aus vier Gründen:

- Über die Sicherheitslücke kann sehr einfach auf die IT-Systeme zugegriffen werden, die Log4j einsetzen. Mit 30-40 Zeichen Befehlscode, kann der Angreifer solche Systeme ausspionieren, die Kontrolle übernehmen und beispielsweise Ransomware aufspielen, um Lösegeld zu erpressen.
- Unglaublich viele Softwarehersteller verwenden die Bibliothek Log4j, denn sie ist Open Source, also kostenfrei verfügbar und ohne Lizenzgebühren nutzbar.
- Log4j wird genutzt, um Zugriffe zu protokollieren, es handelt sich also um eine Verwaltungssoftware mit Wächterfunktion. Und wenn man den Wächter manipulieren kann, ihn ausschalten kann, hat man schnell Zugang zum System – es sei denn, es gibt zusätzliche Sicherungsmaßnahmen.
- Viele Softwarehersteller haben die Bibliothek Log4j einfach ohne weitere Prüfung und ohne zusätzliche Sicherheitsmaßnahmen übernommen – selbst bei IT-Lösungen, die teilsweise in kritischen Infrastrukturen zum Einsatz kommen.

Wo wird Log4j überall eingesetzt?

Weltweit. Das besondere Anwaltspostfach an deutschen Gerichten, musste beispielsweise außer Betrieb genommen werden, jetzt wird dort wieder gefaxt. Bei allen größeren IT-Firmen wird die Bibliothek gern verwendet, also zum Beispiel bei Amazon, Google, IBM, Tesla, Twitter und Cloudflare. Kameraüberwachungssysteme arbeiten ebenfalls damit, QR-Code-Scanner und Smart-Home-Anwendungen wie etwa Türschlösser. Auch sehr viele Konfigurations-Dienstleister, die für andere Unternehmen IT-Systeme aufsetzen und verwalten. Auch in vielen Home Offices findet sich Log4j: Es wird dort eingesetzt, um den WLAN-Zugang zu verwalten. Die fehlerhafte Bibliothek ist also wirklich extrem weit verbreitet.

Gab es denn schon erfolgreiche Angriffe?

Ja. Verschiedene Computer-Notfallteams haben erfolgreiche Angriffe gemeldet, das BSI hat auch einige bestätigt. Allerdings dürften die meisten dieser Zugriffe über diese Sicherheitslücke aktuell von Sicherheitsexperten stammen, die genau nachschauen wollen, wo das Problem liegt. IT-Fachleute gehen davon aus, dass demnächst einige Computernetze über einen Ransomwareangriff lahmgelegt werden, wobei die Ransomware über diese Sicherheitslücke eingeschleust wird. Es gibt Hinweise, dass diese Lücke bereits seit dem 1. Dezember 2021 ausgebnutzt wird. Mittelfristig dürfte deshalb mit einer größeren Welle von Systemausfällen zu rechnen sein.

Wie lassen sich solche Angriffe abwehren?

Die Sicherheitslücke muss zunächst schnell geschlossen werden. Die Hersteller von Softwareprodukten, die die Bibliothek Log4j verwenden, müssen dann Sicherheitsupdates ihrer Software herausgeben. In einigen Fällen ist das am Wochenende bereits passiert, andernorts arbeiten die Hersteller gerade fieberhaft an solchen Updates. Und eine gewisse Anzahl von Herstellern prüft derzeit noch, ob in ihren Produkten eventuell auch Teile aus der Log4j-Bibliothek verwendet wurden. Es wird also noch etwas dauern, bis man Genaueres weiß.

Wie sollten Verbraucher auf die Sicherheitslücke reagieren?

Otto-Normalanwender können zunächst wenig tun. Gefordert sind jetzt die Softwarehersteller und IT-Sicherheitsdienstleister. Als Erste-Hilfe-Maßnahme haben einige Sicherheitsfirmen Filter für Befehlsfolgen gebaut, mit denen die Sicherheitslücke ausgenutzt werde kann. Größere Unternehmen haben bereits am Wochenende die üblichen Notfallmaßnahmen eingeleitet: Zugangsbeschränkungen. Netzwerke aufteilen und segmentieren, so dass nicht sofort das gesamte Unternehmensnetz betroffen ist, wenn solch ein Angriff gelingt, Zugriffsrechte einschränken, ebenso wie hereinkommende Verbindungen und ausführbare Befehle und Programme. Allerdings schränken all diese Maßnahmen natürlich auch die Nutzung der Systeme ein und sind bei den Anwendern wenig beliebt.

Log4J ist Open-Source-Software. Ist die doch nicht so sicher wie gedacht?

Open Source steht dafür, dass jeder draufschauen und Fehler finden kann. Deshalb werden mehr Fehler schneller gefunden. Das heißt aber nicht, dass Open-Source-Software ohne Sicherheitslücken ist. Log4J ist eine quelloffene Software der Apache Software Foundation. Zwei Betreuer werden über Sponsorships in Teilzeit darüber finanziert. Wer also eine solche Bibliothek in Softwareprodukten für kritische Einsatzbereiche verwendet, muss unbedingt genau prüfen, wie sich die Bibliothek in seinem Produkt verhält und nachgeordnete Sicherheitsroutinen einbauen. Doch da wird aus Kostengründen leider gern geschludert. Das ist fahrlässig.

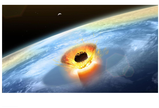
Mehr zum Thema

Archiv

Fehlende IT-Sicherheitsstrategie / Cyberangriffe auf Daten von Corona-Impfstoffen

Archiv

Hacker-Angriffe auf Unternehmen / Erpressungs-Trojaner wurden über Management-Software eingeschleust



Asteroiden-Einschlag / D-Day: Der Anfang vom Ende der Dinosaurier

Entdecken Sie den Deutschlandfunk

Programm
Programm
Alle Sendungen
Die Nachrichten
Nachrichtenleicht
Neue Beiträge auf dlf.de
Themen-Schwerpunkte
Korrekturen

Hören
Livestream
Audios
Podcasts
Apps
Frequenzen

Kontakt
Hörerservice
Social Media

Service
FAQ
Newsletter
Veranstaltungen
Musikliste
RSS

Über uns
Deutschlandradio
Presse
Ausbildung und Karriere
Funkhaus Köln

Deutschlandradio Datenschutzerklärung Nutzungsbedingungen Impressum

Partner ARD ZDF Phoenix arte Chronik der Mauer