Update: Warnstufe Rot: Schwachstelle Log4Shell führt zu extrem kritischer Bedrohungslage (archiviert)

Ort Bonn
Datum 16.12.2021

Quelle: ©olm26250 /iStock Getty Images Plus / Getty Images

Die Schwachstelle namens „Log4Shell" in der weit verbreiteten Java-Bibliothek Log4j führt nach Einschätzung des Bundesamts für Sicherheit in der Informationstechnik (BSI) weiterhin zu einer kritischen IT-Sicherheitslage. Das BSI stellt aktuelle Informationen unter › www.bsi.bund.de/dok/log4j zur Verfügung.

Nach wie vor besteht keine abschließende Klarheit darüber, welche IT-Produkte durch „Log4Shell" verwundbar sind. Einen Überblick über den Verwundbarkeitsstatus zahlreicher IT-Produkte pflegt die niederländische Partnerbehörde des BSI, zu der auch das BSI selbst beiträgt.

Die Schwachstelle wird aktuell mit unterschiedlichen Angriffsformen weltweit ausgenutzt. Neben Angriffen mit Krypto-Minern (dadurch werden die betroffenen Systeme zur Errechnung von Krypto-Währungen missbraucht) oder Bot-Netzen (die betroffenen Systeme werden in Bot-Netze integriert, mit denen bspw. › DDoS-Angriffe durchgeführt werden), sind mittlerweile auch die ersten › Ransomware-Angriffe bekannt geworden. Bei Ransomware-Angriffen werden Computer oder ganze Netzwerke verschlüsselt und die Betroffenen um Lösegeld erpresst.

Aus Sicht des BSI ist mit einer breiten Ausnutzung der Schwachstelle und mit weiteren erfolgreichen Cyber-Angriffen zu rechnen. Diese können auch noch in einigen Wochen und Monaten folgen, wenn die genannte Schwachstelle jetzt für eine Erstinfektion genutzt wird.

Es ist daher weiterhin wichtig, die vom BSI empfohlenen IT-Sicherheitsmaßnahmen schnellstmöglich umzusetzen. Sofern Sicherheits-Updates für verwundbare IT-Produkte zur Verfügung stehen, sollten diese durch alle Anwenderinnen und Anwender eingespielt werden. Daher sind insbesondere Hersteller von IT-Produkten gefordert, ihre Produkte zu prüfen und sie gegebenenfalls durch Sicherheits-Updates abzusichern.

Akut handeln müssen insbesondere Unternehmen und Organisationen und staatliche Stellen auf allen Ebenen. Für diese stehen auch kurzfristige Schutzmaßnahmen zur Verfügung, die die Schwachstelle zwar nicht schließen, ihre Ausnutzung aber verhindern oder erschweren können. Daneben sollten Detektions- und Reaktionsmaßnahmen gestärkt werden.

Verbraucherinnen und Verbraucher sind weniger stark gefährdet, da die fragliche Java-Bibliothek auf Endgeräten weniger stark verbreitet ist. Allerdings können einzelne Anwendungen und smarte Geräte (IoT-Geräte) verwundbar sein. Verbraucherinnen und Verbraucher sind in der Regel darauf angewiesen, dass die Hersteller dieser Produkte entsprechende Sicherheitsmaßnahmen treffen und bspw. Sicherheits-Updates zur Verfügung stellen. Die bestehenden kurzfristigen Schutzmaßnahmen können in der Regel nur von erfahrenen Anwenderinnen und Anwendern umgesetzt werden.

Das BSI wird seine Cyber-Sicherheitswarnung und seine Handlungsempfehlungen fortlaufend aktualisieren. Das Nationale IT-Krisenreaktionszentrum im BSI bleibt weiterhin aktiv. Das BSI steht in intensivem Austausch mit nationalen und internationalen Partnern.

Vorangegangene Pressemitteilung

Bonn, 11.12.2021. Die kritische Schwachstelle (Log4Shell) in der weit verbreiteten Java-Bibliothek Log4j führt nach Einschätzung des Bundesamts für Sicherheit in der Informationstechnik (BSI) zu einer extrem kritischen Bedrohungslage. Das BSI hat daher seine bestehende Cyber-Sicherheitswarnung auf die Warnstufe Rot hochgestuft. Ursächlich für diese Einschätzung ist die sehr weite Verbreitung des betroffenen Produkts und die damit verbundenen Auswirkungen auf unzählige weitere Produkte. Die Schwachstelle ist zudem trivial ausnutzbar, ein Proof-of-Concept ist öffentlich verfügbar. Eine erfolgreiche Ausnutzung der Schwachstelle ermöglicht eine vollständige Übernahme des betroffenen Systems. Dem BSI sind welt- und deutschlandweite Massen-Scans sowie versuchte Kompromittierungen bekannt. Auch erste erfolgreiche Kompromittierungen werden öffentlich gemeldet.

Das ganze Ausmaß der Bedrohungslage ist nach Einschätzung des BSI aktuell nicht abschließend feststellbar. Zwar gibt es für die betroffene Java-Bibliothek Log4j ein Sicherheits-Update, allerdings müssen alle Produkte, die Log4j verwenden, ebenfalls angepasst werden. Eine Java-Bibliothek ist ein Software-Modul, das zur Umsetzung einer bestimmten Funktionalität in weiteren Produkten verwendet wird. Es ist daher oftmals tief in der Architektur von Software-Produkten verankert. Welche Produkte verwundbar sind und für welche es bereits Updates gibt, ist derzeit nicht vollständig überschaubar und daher im Einzelfall zu prüfen. Es ist zu erwarten, dass in den nächsten Tagen weitere Produkte als verwundbar erkannt werden.

Das BSI empfiehlt insbesondere Unternehmen und Organisationen, die in der Cyber-Sicherheitswarnung skizzierten Abwehrmaßnahmen umzusetzen. Darüber hinaus sollten die Detektions- und Reaktionsfähigkeiten kurzfristig erhöht werden, um die eigenen Systeme angemessen überwachen zu können. Sobald Updates für einzelne Produkte verfügbar sind, sollten diese eingespielt werden. Darüber hinaus sollten alle Systeme auf eine Kompromittierung untersucht werden, die verwundbar waren.

Pressekontakt:

Bundesamt für Sicherheit in der Informationstechnik
Pressestelle
Tel.: 0228-999582-5777
E-Mail: presse@bsi.bund.de
Internet: › www.bsi.bund.de

› BSI in Social Media

Weitere Informationen

- Download Version 1.2: Kritische "Log4Shell" Schwachstelle in weit verbreiteter Protokollierungsbibliothek Log4j (PDF)
- Kritische Schwachstelle in Java-Bibliothek log4j
- Arbeitspapier Detektion und Reaktion Log4j Schwachstelle, Version 1.4
- DDoS
- Ransomware

© Bundesamt für Sicherheit in der Informationstechnik