Kritische Schwachstelle in Java-Bibliothek Log4j

Die kritische Schwachstelle CVE-2021-44228 [MIT2021] (Log4Shell) sowie zwei weitere Schwachstellen (CVE-2021-45046, CVE-2021-45105) in der weit verbreiteten Java-Bibliothek Log4j führten nach Einschätzung des BSI Mitte Dezember 2021 zunächst zu einer extrem kritischen Bedrohungslage. Diese hat sich nach Ansicht des BSI deutlich entspannt. Das BSI hat daher die Warnstufe der **Cyber-Sicherheitswarnung (CSW 2021-549177-1232) am 12.01.2022** von Rot auf Gelb herabgesetzt.

Eine Vielzahl von Softwareherstellern hat inzwischen Patches oder Workarounds für ihre Produkte veröffentlicht. Die erwartete Ausnutzung der Schwachstelle über die Weihnachtsferien 2021 trat in Deutschland nicht ein. Es bestehen allerdings Hinweise darauf, dass die Schwachstelle international ausgenutzt wird. Die Patches oder Workarounds sollten mittlerweile von Unternehmen und Behörden eingespielt und die Netze auf mögliche Ausnutzung im Verwundbarkeitszeitfenster geprüft worden sein.

Detektion und Reaktion

Das **Arbeitspapier Detektion und Reaktion Log4j Schwachstelle, Version 1.4** fasst detaillierte Informationen zu den bisher bekannten Schwachstellen, möglichen Mitigationsmaßnahmen sowie geeigneten Detektionsmaßnahmen zusammen.

Bisherige Meldungen des BSI

Version 1.2: Kritische "Log4Shell" Schwachstelle in weit verbreiteter Protokollierungsbibliothek Log4j (12.01.2022)
Zur Verbesserung der Übersichtlichkeit und Lesbarkeit wurden am 14.12.2021 alle Erkenntnisse in einer CSW konsolidiert. Diese CSW mit der Nummer 2021-549177-1032 ersetzt daher die CSW 2021-549032-1432.

Version 1.5: Kritische Schwachstelle in log4j veröffentlicht
(Diese CSW mit Nummer 2021-549032-1432 wird nach dem Update 1.5 vom 17.12.2021 nicht weiter aktualisiert.)

Pressekonferenz am 13.12.2021, 15 Uhr (Stream der Tagesschau)

Pressemitteilung vom 11.12.2021

Empfehlungen für Verbraucherinnen und Verbraucher

Java-Bibliothek Log4j – eine Bilanz

Sicherheitslücke "Log4Shell" gefährdet Systeme weltweit

Kurzinformationen von CERT-Bund

Der Warn- und Informationsdienst (WID) von **CERT-Bund** führt von aktuellen Sicherheitslücken und Schwachstellen betroffene Software-Produkte sowie zugehörige Quellen auf. Diese Kurzinformationen richten sich in erster Linie an IT-Kräfte in Bundesverwaltung, KRITIS-Unternehmen und CERTs, können aber auch von Bürgerinnen und Bürger abonniert werden. Diese Informationen sind teilweise nicht verifiziert und daher unter Umständen unvollständig oder fehlerhaft.

Die aktuellste Kurzinformation zu Log4j:

Risikostufe	Titel	Datum

Weitere Informationen und personalisierte Abonnements gibt es auf der Website des **Warn- und Informationsdienstes (WID)**.

Kurz-URL: https://www.bsi.bund.de/dok/log4j

Seite drucken