21 Dez. 2021 -09:10

Das Zentrum für Cybersicherheit Belgien erwartet große Probleme für Unternehmen und Organisationen, die keine Maßnahmen gegen die Log4j-Schwachstelle ergreifen

Unternehmen, die Apache Log4j-Software einsetzen und noch keine Maßnahmen ergriffen haben, müssen in den kommenden Tagen und Wochen mit erheblichen Problemen rechnen. Diese Sicherheitslücke wird von Cyberkriminellen aktiv ausgenutzt. Wer nicht handelt, kann sehr schnell Opfer eines Cyberangriffs werden.

Letzte Woche wurde eine Sicherheitslücke in Apache Log4j entdeckt. Dabei handelt es sich um Software, die häufig in Webanwendungen und allen möglichen anderen Systemen eingesetzt wird. Die Sicherheitslücke ermöglicht es Angreifern, die Rechte von entfernten Webservern zu missbrauchen. Da diese Software so weit verbreitet ist, lässt sich nur schwer abschätzen, wie und in welchem Umfang die entdeckte Schwachstelle ausgenutzt werden wird. In der Zwischenzeit versuchen Cyberkriminelle, die Schwachstelle auszunutzen und suchen aktiv nach anfälligen Systemen. Es versteht sich von selbst, dass dies eine gefährliche Situation ist. Updates sind bereits verfügbar.

Das Zentrum für Cybersicherheit Belgien (CCB) rät daher den Nutzern von Apache Log4j, die verfügbaren Updates so schnell wie möglich zu installieren. Bitte beachten Sie diese technischen Hinweise. Wenn Sie nicht sicher sind, ob Apache Log4j in Ihrer Organisation verwendet wird, fragen Sie Ihren Softwarelieferanten.

Das Zentrum beobachtet die Situation genau und wird neue Informationen veröffentlichen, sobald sie verfügbar sind.

Unternehmen und Organisationen, die Opfer eines Cyberangriffs werden, können dies unter cert@cert.be melden.

Zentrum für Cybersecurity Belgien
Rue de la Loi 18
1000 Brüssel
Belgien
http://www.ccb.belgium.be

Katrien - Eggers
Kommunikationsberaterin
+32 485 76 53 36
katrien.eggers@cert.be