21 déc 2021 -09:10

Le Centre pour la Cybersécurité Belgique prévoit des problèmes majeurs pour les entreprises et les organisations qui ne prennent pas de mesures contre la vulnérabilité de Log4j

Les entreprises qui utilisent le logiciel Apache Log4j et qui n'ont pas encore pris de mesures peuvent s'attendre à des problèmes majeurs dans les jours et les semaines à venir. Cette vulnérabilité est activement exploitée par les cybercriminels. Ceux qui ne prennent pas de mesures peuvent très vite être victimes d'une cyberattaque.

La semaine dernière, une vulnérabilité a été découverte dans Apache Log4j. Il s'agit d'un logiciel qui est souvent utilisé dans les applications web et toutes sortes d'autres systèmes. La vulnérabilité permet aux attaquants d'abuser des droits des serveurs web distants. Ce logiciel étant très largement distribué, il est difficile d'estimer comment la vulnérabilité découverte sera exploitée et à quelle échelle. Les mises à jour sont actuellement disponibles.

Le Centre pour la Cybersécurité Belgique (CCB) conseille donc aux utilisateurs d'Apache Log4j d'installer les mises à jour disponibles dès que possible. Veuillez suivre ces conseils techniques. Si vous ne savez pas si Apache Log4j est utilisé dans votre organisation, demandez à votre fournisseur de logiciels.

Le CCB suit de près la situation et publiera de nouvelles informations sur les mises à jour dès qu'elles seront disponibles.

Les entreprises et les organisations qui sont victimes d'une cyberattaque peuvent le signaler à cert@cert.be.

Centre pour la Cybersécurité Belgique
Rue de la Loi 18
1000 Bruxelles
Belgique
http://www.ccb.belgium.be

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