04 juil 2021 -15:01

Désactivez Kaseya VSA : vous risquez une attaque de ransomware suite à l'attaque 'Supply Chain' sur l'entreprise de logiciels Kaseya

Menace mondiale des attaques ransomware:

- Une attaque Supply Chain est une attaque contre un partenaire externe, tel qu'un vendeur ou un fournisseur, qui a accès à votre réseau.
- Kaseya, un fournisseur de logiciels informatiques, a été victime d'une attaque Supply Chain. Les pirates ont réussi à compromettre Kaseya VSA, un logiciel qui permet la gestion à distance des systèmes, pour attaquer les utilisateurs de ce logiciel.
- Les clients de Kaseya utilisant le produit VSA pourraient être visés par une variante du ransomware REvil.
- CERT.be, le service opérationnel du Centre de la Cybersécurité Belgique (CCB), a averti le 3 juillet les utilisateurs de Kaseya VSA de désactiver temporairement le produit jusqu'à ce que davantage d'informations soient disponibles.
- Il n'y a actuellement aucune victime belge connue. Le CCB suit de près la situation.

Les agences gouvernementales et les entreprises belges sont-elles en danger?

Le logiciel Kaseya VSA est utilisé dans le monde entier, y compris en Belgique. La CCB ne connaît pas tous ses clients belges et n'a pas reçu à ce jour de signalement concernant une victime belge. Cependant, il est toujours important de surveiller cette menace et de rechercher et aider les victimes potentielles.

Qu'a fait le Centre pour la Cybersécurité Belgique (CCB) ?

Le CCB a pris cette menace au sérieux dès le début. Le 3 juillet, CERT.be, le département opérationnel du CCB, a envoyé un avertissement et des conseils aux utilisateurs de Kaseya VSA.

- Suivez les conseils de Kaseya et désactivez toutes les instances du serveur Kaseya VSA, au moins jusqu'à ce que plus d'informations soient disponibles.
- Les organisations qui fournissent Kaseya VSA doivent informer leurs clients de cette menace et prendre les mesures appropriées.
- Les utilisateurs de Kaseya VSA doivent renforcer leurs capacités de surveillance et de détection des activités suspectes afin de pouvoir réagir rapidement en cas d'intrusion.

https://cert.be/nl/alert/warning-imminent-threat-ransomware-operators-are-exploiting-kaseya-supply-chain-

attack

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

Andries Bomans
Responsable communication
+32 471 66 00 06
andries.bomans@ccb.belgium.be

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