Kaseya : ce patch qu'on attend toujours

Le grand redémarrage de VSA ? Ça ne devrait pas être avant dimanche 11 juillet. Soit quasiment une semaine après la date de reprise initialement estimée. Kaseya, l'éditeur de ce logiciel de gestion informatique, préfère prendre son temps pour diffuser le correctif censé éliminer la faille où s'est engouffré le *ransomware* REvil.

En attendant le patch, les clients sont invités à se préparer. En première ligne, les installations sur site. Pour elles, la *checklist* va de l'isolation des serveurs à l'implémentation d'un agent antivirus. En l'occurrence, celui de FireEye Endpoint Security, pour lequel Kaseya va fournir des licences.

Pour la version SaaS, la restauration avait démarré le 6 juillet au soir. Mais quelques heures plus tard, machine arrière. Kaseya affirmait avoir identifié « un problème » pendant le déploiement. Dans ce contexte, il a décidé de mettre en place des couches de sécurité supplémentaires. Dont, pour chaque instance de VSA, un SOC et un CDN complémentaire avec WAF (sur *opt-in* pour les versions *on-prem*). Ainsi qu'un changement d'IP pour les serveurs hébergeant la version SaaS (révision à prévoir, donc, pour qui utilise un *firewall* avec liste blanche).

Au-delà de colmater la vulnérabilité, le correctif supprimera les fonctionnalités ci-contre. Il suspendra par ailleurs, sur la version SaaS, tous les agents. Kaseya recommande de les réactiver progressivement, « par groupe de 10 à 15 ».

> *UPDATE: @RonanKirby, President & General Manager EMEA at @KaseyaCorp confirmed to give a short presentation about the « Ongoing Incident Response ». This extra talk has a minor impact on the original agenda. #CCBQCTR #cybersecurity #Kaseya https://t.co/3jYEkPNPMI https://t.co/oz6yzRpLX2*
>
> *— CERT.be (@certbe) July 7, 2021*

Photo d'illustration © Skórzewiak – Adobe Stock